TCI
RECHTSANWÄLTE

Abschrift

TCI Partnerschaft von Rechtsanwälten Müller Schmidt
Fasanenstr. 61 · D - 10719 Berlin

Vorab per Fax 9023-2223

Landgericht Berlin
Zivilkammer 57

10617 Berlin

EINGEGANGEN
03. Dez. 2012
Erl.

TCI Partnerschaft von
Rechtsanwälten Müller Schmidt
Fasanenstr. 61
D - 10719 Berlin
Tel: +49 - (0)30 - 20 05 42-0
Fax: +49 - (0)30 - 20 05 42-11
www.tcilaw.de

Norman Müller
Markus Schmidt
Carsten Gerlach

In Kooperation mit
TCI Rechtsanwälte München
Ruth Dünisch
Dr. Truiken J. Heydn
Dr. Michael Karger [1,2]
Harald Krüger [3]
Dr. Andreas Stadler
Dr. Thomas Stögmüller [1]
LL.M. (Berkeley)

TCI Rechtsanwälte Mainz
Stephan Schmidt [1]
Sabine Brumme
Stephan Breckheimer
LL.M. (Medienrecht)
Dr. Olaf Griebenow

Fachanwalt für
[1] Informationstechnologierecht
[2] Verwaltungsrecht
[3] Arbeitsrecht

Berlin, den 30. November 2012

Ansprechpartn[redacted]
E-Mail-Adresse:
Aktenzeichen: 172/00123-08/ms

In dem Rechtsstreit
Patrick Breyer ./. Bundesrepublik Deutschland
- 57 S 87/08 -

bedanken wir uns zunächst für die gewährte Fristverlängerung.

1. Privatgutachten zum Beweisbeschluss vom 20. Mai 2010

Wir überreichen zunächst das Privatgutachten von Herrn Prof. Martini als

Anlage BB 5 (nachfolgend als Privatgutachten bezeichnet).

1.1 Zur Person des Gutachters

Herr Professor Martini ist Leiter des Instituts für Informatik IV (Kommunikation und vernetzte Systeme) der Universität Bonn und Leiter des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie.

Sitz der Gesellschaft: Berlin - Amtsgericht Charlottenburg – PR 784
HypoVereinsbank Berlin (BLZ 100 208 90) Konto-Nr. 20 35 92 69
IBAN: DE39 1002 0890 0020 3592 69 – SWIFT/BIC: HYVEDEMMXXX
USt-IdNr. DE815371100 - Steuernummer: 24/555/00297

Das Institut für Informatik IV der Universität Bonn ist u. a. spezialisiert auf die praxisorientierte Forschung im Bereich der Sicherheit und Effizienz im Internet. Ein Forschungsschwerpunkt des Instituts liegt also explizit im Bereich der mit dem Beweisbeschluss des Landgerichtes vom 20. Mai 2010 aufgeworfenen Fragen zur Sicherheit von IT-Systemen im Internet.

Beweis: Darstellung der Forschungsschwerpunkte des Instituts für Informatik IV der Universität Bonn, **Anlage BB 6**

Herr Professor Martini gehört damit zu den führenden Experten für IT-Sicherheit im Bereich des Internets.

1.2 Zusammenfassung der Feststellungen des Gutachters

Der Gutachter kommt in seinem Privatgutachten zu fundamental anderen Feststellungen als der gerichtlich beauftragte Sachverständige Dr. Köpsell.

Zusammenfassend werden die Fragen des Beweisbeschlusses durch den Gutachter Prof. Martini wie folgt beantwortet:

1. Die Speicherung von IP-Adressen entspricht zentralen international anerkannten Richtlinien für den Betrieb von Webservern und damit dem nationalen und internationalen Stand der Technik. Sie dient darüber hinaus dem Stand der Technik als unverzichtbares Element bei der technischen Weiterentwicklung von Abwehrmaßnahmen.

2. Die Speicherung von IP-Adressen ist zum Schutz von Webseiten gegen schadhafte Angriffe und zur Minderung der Gefahr von Sicherheitsverletzungen unverzichtbar und kann nicht durch andere Maßnahmen ersetzt werden.

3. Die Kosten für mögliche Alternativmaßnahmen sind nicht bezifferbar, da es keine tauglichen Alternativmaßnahmen gibt.

Beweis: Privatgutachten des Herrn Prof. Martini, **Anlage BB 5**

Nachfolgend wird auf eine ausführliche schriftsätzliche Wiederholung des Privatgutachtens verzichtet. Es werden vielmehr nur noch einmal die Kernaussagen des Privatgutachtens zu den drei Beweisfragen des Landgerichts kurz dargestellt. Im Übrigen verweisen wir auf den Inhalt des Privatgutachtens. Sollte das Gericht diese pauschale Bezugnahme für unzulässig erachten und eine detailliertere schriftsätzliche Darstellung des Inhalts des Privatgutachtens für erforderlich halten, bitten wir um einen entsprechenden richterlichen Hinweis.

1.3 Beweisfrage 1

Die Speicherung der IP-Adressen dient nach den Feststellungen des Privatgutachtens dem Stand der Technik insbesondere dadurch, dass nur auf Basis der Erkennung und Analyse erfolgreicher Angriffe für die Zukunft geeignete Abwehrmaßnahmen gegen die entsprechenden Angriffe entwickelt werden können. Wesentlicher Ansatzpunkt für eine erfolgreiche Erkennung und Analyse ist dabei die Analyse der IP-Adressen, von der aus auf die kompromittierten Systeme zugegriffen wurde. Die IP-Adressen sind hierbei ein unverzichtbares Datum. Anders ausgedrückt: Ohne Analyse der IP-Adressen sind sowohl die Angriffserkennung als auch die Angriffsanalyse nicht oder nur sehr eingeschränkt möglich. Die Entwicklung von vorbeugenden Schutzmaßnahmen gegen entsprechende Angriffe wäre damit massiv behindert, wenn nicht gar verhindert.

Das Privatgutachten weist weiter darauf hin, dass die Speicherung der IP-Adressen in den international anerkannten amerikanischen „Guidelines on Securing Public Web Servers“ des National Institute of Standards and Technology ausdrücklich empfohlen wird, um Web-Server erfolgreich zu schützen. Der Gutachter Prof. Martini kommt daher zu der eindeutigen Feststellung, dass die Speicherung der IP-Adressen für den sicheren Betrieb von Web-Servern in anerkannten Richtlinien und Standards empfohlen wird und daher dem Stand der Technik entspricht.

1.4 Beweisfrage 2

Das Privatgutachten legt anschaulich dar, dass allein vorbeugende Maßnahmen zum Schutz von IT-Systemen für Telemedien nicht ausreichend sind. Vielmehr sind auch reaktive Maßnahmen notwendig, um u. a. eine wirkungsvolle Angriffserkennung, eine Schadensanalyse erfolgreicher Angriffe, eine aus der Erkennung und Analyse von Angriffen abgeleitete Verbesserung vorbeugender Abwehrmaßnahmen und eine Unterrichtung möglicherweise betroffener Dritter vornehmen zu können und nicht zuletzt auch um eine Verfolgung von Angreifern auch nur ansatzweise zu ermöglichen und damit überhaupt eine Generalprävention zur Vermeidung von Angriffen vorzunehmen. Ein unverzichtbarer zentraler Ansatzpunkt für entsprechende reaktive Maßnahmen ist die Analyse der IP-Adressen, von denen aus Zugriffe auf kompromittierte Systeme erfolgt sind.

Nach den Feststellungen des Privatgutachtens würde die vom Sachverständigen Dr. Köpsell als Alternative angeführte Pseudonymisierung der IP-Adressen die IP-Adressen für diese Zwecke nach derzeitigem Stand der Technik unbrauchbar machen. In wissenschaftlichen Forschungsarbeiten verschiedentlich aufgeführte Methoden der Pseudonymisierung sind für den praktischen Einsatz zur effektiven Angriffserkennung und –abwehr heute und auf absehbare Zeit nicht geeignet.

Weitere alternative Maßnahmen, die die Speicherung der IP-Adressen ersetzen und gleichwohl die erforderlichen reaktiven Schutzmaßnahmen ermöglichen, konnte der Sachverständige Dr. Köpsell nicht ansatzweise benennen. Alle weiteren Ausführungen des Sachverständigen insbesondere in seiner ergänzenden Stellungnahme zielen ausschließlich auf vorbeugende Maßnahmen, welche für sich alleine aber nach den nachvollziehbaren Erwägungen des Privatgutachtens für einen sicheren Betrieb der IT-Systeme nicht ausreichend sind.

1.5 Beweisfrage 3

Die Antwort auf diese Beweisfrage enthält die einzig logische Konsequenz auf die Feststellungen des Gutachters zu den Beweisfragen 1 und 2. Nach den Feststellungen des Gutachters ist die Speicherung der IP-Adressen für einen si-

cheren Betrieb der Telemedien der Beklagten bei dem heutigen Stand der Technik unverzichtbar und kann auch auf absehbare Zeit nicht durch andere Maßnahmen, insbesondere nicht durch die vom Sachverständigen Dr. Köpsell angeführte Pseudonymisierung ersetzt werden.

2. Stellungnahme zu den Erläuterungen des Sachverständigen Dr. Köpsell vom 7. Mai 2012

2.1 zu Beweisfrage 3

Die vom Sachverständigen nunmehr nachgereichte Begründung für die Nichtbeantwortung der Beweisfrage 3 ist mehr als dürftig. Der Sachverständige beruft sich zunächst darauf, dass ihm die zur Beantwortung dieser Frage erforderlichen Informationen über die zu schützenden Systeme fehlen würden. Hierzu ist festzuhalten, dass der Sachverständige, wie er selber einräumt, bereits keinerlei Versuch unternommen hat, diese Informationen zu erhalten. Darüber hinaus beruft er sich darauf, dass das im Rahmen des Gutachtensauftrags genannte Budget für das Gutachten eine Beantwortung dieser Frage nicht zuließe. Auch hierzu muss sich der Sachverständige vorhalten lassen, dass er den Gutachtensauftrag in Kenntnis des Budgets und in Kenntnis der zu beantwortenden Fragen angenommen hat.

Abgesehen von der eigentlich damit bestehenden zivilrechtlichen Verpflichtung des Sachverständigen, den angenommenen Auftrag in vollem Umfang zu erfüllen, stellt sich die Frage, warum der Sachverständige nicht bereits vorher dieses Problem gegenüber dem Gericht aufgeworfen hat. In Anbetracht seiner Bearbeitungszeit für das Gutachten wäre hierzu jedenfalls ausreichend Gelegenheit gewesen. Die Ausführungen des Sachverständigen hierzu müssen daher als reine Ausflüchte und Schutzbehauptungen gesehen werden. Der Sachverständige scheint entweder fachlich nicht in der Lage zu sein, die Beweisfrage zu beantworten, da ihm, wie beklagtenseitig bereits von Anfang an befürchtet, die erforderlichen praktischen Erfahrungen beim Schutz hochsensibler IT-Systeme im Internet fehlen oder – zu berücksichtigen ist hier, dass der Sachverständige vom Kläger vorgeschlagen wurde und der Kläger von Anbeginn

des Verfahrens bemüht war, sein finanzielles Prozessrisiko möglichst gering zu halten – die Kosten für das Sachverständigengutachten gering gehalten werden sollten, um das Prozessrisiko für den Kläger gering zu halten.

2.2 zu Beweisfrage 2

Zur Vermeidung von Wiederholungen soll nachfolgend nur noch auf ausgewählte Punkte der Stellungnahme des Sachverständigen eingegangen werden. Es verbleibt im Übrigen in vollem Umfang bei unseren Anmerkungen aus unserem Schriftsatz vom 26. Oktober 2011, die in keiner Weise durch die ergänzende Stellungnahme widerlegt, im Gegenteil sogar eher noch bestätigt werden. Die Ausführungen sind weiterhin in sich widersprüchlich und die „Ergebnisse" nicht durch die weiteren Ausführungen gedeckt. Der Sachverständige ist offensichtlich zu einer fundierten, in sich logischen Beantwortung der Beweisfrage nicht in der Lage. Er erfindet daher Sachverhalte, wie z. B. die Sachverhaltsunterstellung, die Speicherung der IP-Adresse sei die einzige Maßnahme der Beklagten zur Angriffsabwehr und zieht aus diesem erfundenen Sachverhalt seine Schlüsse und Ergebnisse.

2.2.1 zu Anmerkung 2.2

Die Erklärungen des Sachverständigen an dieser Stelle sind nicht nachvollziehbar. Er besteht darauf, dass eine IP-Adresse frei gewählt werden könne und deshalb eine Speicherung von IP-Adressen gar keinen Sinn mache. Gleichzeitig muss er aber einräumen, dass bei freier Wahl der IP-Adresse keine oder eine nur eingeschränkte Kommunikation möglich sei. Diese Aussage ist etwa so sinnvoll, wie die Aussage, dass man auch mit einem ausgeschalteten Mobiltelefon telefonieren könne. Selbstverständlich kann man auch in ein ausgeschaltetes Gerät hineinsprechen und wenn der Gesprächspartner nah genug ist, erreicht die Kommunikation auch ihren Empfänger. Welchen Sinn dies allerdings machen soll, ist hier nicht ersichtlich. Der Regelfall moderner Angriffsszenarien, die häufig gerade auf Kommunikation basieren, ist damit jedenfalls nicht beschrieben. Insoweit verbieten sich auch verallgemeinernde Schlussfolgerungen daraus.

Im Übrigen weisen wir auf Seite 19 letzter Absatz des Privatgutachtens hin. Danach werden heute gefälschte IP-Absender-Adressen (IP-Spoofing) von seriösen Providern ausgefiltert. Der Sachverständige kann deshalb auch nur auf ein Angriffsszenario aus den 90er Jahren und damit der Steinzeit des Internet verweisen. Moderne Angriffsszenarien bauen dagegen, wie im Privatgutachten anschaulich dargestellt, sehr häufig gerade auch auf der Kommunikation zwischen angreifendem und angegriffenem System auf.

Ob diese Angriffe ausschließlich von „Dummen" im Sinne der Definition des Sachverständigen ausgeführt werden, soll der Beurteilung des Sachverständigen überlassen bleiben. Tatsache ist jedenfalls, dass die im Privatgutachten genannten Angriffe eine ernsthafte Bedrohung darstellen, gegen die alle geeigneten Sicherheitsvorkehrungen getroffen werden müssen. Hierzu zählt, wie das Privatgutachten belegt, in jedem Fall auch die Speicherung der IP-Adressen.

Die Ausführungen des Sachverständigen zur möglichen Fälschung von IP-Adressen sind insofern ohne jegliche Aussagekraft.

2.2.2 zu Anmerkung 2.4

Der Sachverständige räumt in seiner Stellungnahme selbst ein, dass für einen wirksamen Firewallschutz dort kompromittierte IP-Adressen gespeichert werden müssen, um erneute Anfragen von diesen IP-Adressen abweisen zu können. Anschließend differenziert er dann zwischen dieser „guten" Speicherung von IP-Adressen und einer anderen „bösen" Speicherung. Eine solche Differenzierung ist weder Gegenstand der Beweisfrage noch differenziert der Unterlassungsantrag des Klägers insoweit. Die Ausführungen des Sachverständigen gehen daher an der Beweisfrage vorbei.

Dies gilt ebenfalls für seine weiteren Ausführungen. Der Sachverständige spekuliert hier über die Motivation des Klägers. Diese Spekulationen finden jedoch weder einen Ansatzpunkt im Beweisbeschluss, noch in den Anträgen des Klägers. Der Kläger begehrt schlicht das Unterlassen der Speicherung der IP-Adresse gleichgültig wo, in welchem Zusammenhang und in welchem Datenkontext diese Speicherung erfolgt.

Was schließlich die vom Sachverständigen vorgeschlagene Ersetzung der IP-Adresse anbelangt, erläutert das Privatgutachten ausführlich, warum ein solches Vorgehen technisch ungeeignet ist, einen zur Speicherung der originären IP-Adresse vergleichbaren Schutz herbeizuführen.

2.2.3 zu Anmerkung 2.3

Wie sich aus dem Privatgutachten ergibt, ist der Vorschlag des Sachverständigen zur Ersetzung der IP-Adresse aus vielerlei Gründen ungeeignet. Es kann daher dahingestellt bleiben, ob die vom Sachverständigen favorisierte Pseudonymisierung tatsächlich dem vom Kläger geforderten vollständigen Verzicht auf die Speicherung der IP-Adresse genügen würde. Da der Kläger offensichtlich einem fundamentalistisch abstrakten Bestimmbarkeitsbegriff anhängt, dürfte ihm eine auch nur potenziell rückführbare Pseudonymisierung nicht ausreichen. Jedenfalls wäre es der Beklagten nicht zumutbar, sich im Falle eines klagestattgebenden Urteils darauf verlassen zu müssen, dass der Kläger und/oder ein Gericht in einem anschließenden Ordnungsmittelverfahren den Bestimmbarkeitsbegriff zu Gunsten der Beklagten auslegen würde. Insoweit sind also auch hier die Ausführungen des Sachverständigen nicht zielführend und stellen gerade keine verlässliche Alternative zur Speicherung der IP-Adresse dar.

2.2.4 zu Anmerkung 2.5

Wie die Ausführungen von Prof. Martini in seinem Privatgutachten zeigen, ist die Information potentiell von Bot-Netzen betroffener Privatpersonen gerade nicht, wie vom Sachverständigen Dr. Köpsell behauptet, unrealistisch, sondern vielmehr ist der Sachverständige auch an dieser Stelle schlicht nicht sachverständig. Natürlich kann die Beklagte mangels Kenntnis der Zuordnung der IP-Adressen nicht selbst die Betroffenen unterrichten. Die Beklagte kann aber den Providern die fraglichen IP-Adressen übermitteln, so dass diese ihre Kunden entsprechend unterrichten können, was in der Vergangenheit offensichtlich so auch bereits praktiziert wurde und nach wie vor wird.

2.2.5 zu Anmerkung 2.6

Es kann völlig dahingestellt bleiben, welche Maßnahmen in dem vom Sachverständigen angeführten Anonymisierungsdienst zum Schutz des IT-Systems vor Angriffen ausgeführt werden. Es handelt sich bei diesem System um ein kleines, mit den Systemen der Beklagten nicht vergleichbares System. Dies zeigt allein der Umstand, dass genau ein Benutzer, nämlich der Administrator eingerichtet ist. Es bedarf wohl keiner weiteren Erläuterung, dass die Beklagte ihre Web-Server nicht mit ausschließlich einem Benutzer administrieren und verwalten kann. Dies mag für einen statischen Anonymisierungsdienst möglich sein, nicht aber für Webdienste, über die tausende, im Zweifel fortlaufend zu aktualisierende Einzelinformationen angeboten werden.

Weitgehend disqualifiziert sich der Sachverständige im Übrigen selbst, wenn er für ein gängiges Firewall-System auf das Betriebssystem Windows 7 verweist. Es bleibt zu hoffen, dass auch dem Sachverständigen klar ist, dass Windows 7 kein gängiges Produkt zum Schutz von IT-Systemen, sondern ein Betriebssystem mit einigen rudimentären Schutzfunktionen darstellt. Jedenfalls dürfte ein IT- System, dass hinsichtlich der eingesetzten Firewall zum Schutz vor Angriffen ausschließlich auf das Produkt Windows 7 setzt, nach im Übrigen einhelliger Meinung der Fachwelt nicht als sicher gelten.

2.2.6 zu Anmerkung 2.7

An dieser Stelle offenbart der Sachverständige einmal mehr seine erheblichen Logikdefizite. Er kommt zu dem Schluss, dass Maßnahmen zur Generalprävention generell nicht erforderlich seien, weil man Angreifer aus Drittstaaten möglicherweise nicht verfolgen könne und dort daher die Generalprävention nicht wirke. Stattdessen müssten andere Schutzmaßnahmen ergriffen werden. Der Sachverständige meint also offensichtlich, Maßnahmen zur Generalprävention seien nur dann sinnvoll, wenn sie sämtliche potentiellen Täter abhalten würden. Dies ist erkennbarer Unsinn.

Wie an vielen Stellen des Sachverständigengutachtens und der ergänzenden Stellungnahme des Sachverständigen beruht seine Argumentation auch hier darauf, dass eine Maßnahme (hier konkret die Speicherung von IP-Adressen) nicht erforderlich, sondern allenfalls nützlich ist, wenn sie für sich alleine nicht geeignet ist, jegliche Angriffe auf IT-Systeme bzw. die Web-Server der Beklagten zu unterbinden. Gleichzeitig muss

er aber selbst einräumen, dass es einhundertprozentigen Schutz und Sicherheit nicht gibt. Folgt man der Logik des Sachverständigen, kann dies also nur bedeuten, dass überhaupt keine Maßnahme erforderlich ist, weil ja keine einzelne Maßnahme völligen Schutz bietet (nicht einmal die Gesamtheit aller denkbaren Maßnahmen). Die Unlogik dieser Schlussfolgerung liegt auf der Hand.

2.3 zu Beweisfrage 1

Mit seiner Stellungnahme nimmt der Sachverständige nunmehr offensichtlich selbst die eindeutig negative Beantwortung der Beweisfrage in der Zusammenfassung seines Gutachtens zurück und führt nunmehr aus, dass die Frage – jedenfalls von ihm – nicht beantwortet werden kann. Dem ist nichts hinzuzufügen. Im Übrigen verweisen wir auf die eindeutigen Aussagen im Privatgutachten.

3. Rechtslage

Unabhängig von den oben diskutierten technischen Fragen und einer daraus resultierenden Rechtfertigung eines Eingriffs in mögliche Rechte des Klägers fehlt es jedoch bereits an einer Rechtsverletzung auf Seiten des Klägers. Im Hinblick auf diese Rechtsfrage haben sich seit dem Verfahrensbeginn erhebliche Entwicklungen in Rechtsprechung, Literatur und auch der Gesetzgebung ergeben.

3.1 Ausgangslage

Unstreitig ist, dass der Kläger für die Nutzung der Internetangebote der Beklagten eine dynamische IP-Adresse nutzt, d. h. die jeweilige IP-Adresse wird dem Kläger durch seinen Provider jeweils für eine Internetnutzung neu zugewiesen. Die Zuordnung einer solchen dynamischen IP-Adresse zu dem Anschlussinhaber, von dessen Telekommunikationsanschluss der jeweilige Internetzugriff erfolgt ist, kann nur durch den Provider des Anschlussinhabers erfolgen. Für Dritte, wie die Beklagte ist eine solche Zuordnung dagegen nicht möglich, da sie über die dafür notwendigen Informationen des Providers nicht verfügt. Eine eindeutige Zuordnung zu einem konkreten Nutzer ist ohnehin

nicht möglich, da die IP-Adresse nur den Anschlussinhaber bzw. das dort angeschlossene Endgerät identifiziert, nicht aber den konkreten Nutzer, d. h. die natürliche Person, die das jeweilige Endgerät nutzt.

3.2 Entwicklung in der Rechtsprechung

Mit Beschluss vom 3. November 2010 (Az. 5 W 126/10) hat das OLG Hamburg eindeutig festgestellt, dass dynamische IP-Adressen für Dritte, d. h. alle außer dem Provider, keine personenbezogenen Daten darstellen.

Der Bundesgerichtshof hat in seiner Entscheidung vom 12. Mai 2010 (Az. I ZR 121/08) ebenfalls festgestellt, dass einer IP-Adresse keine Identifikationsfunktion zukommt und damit kein personenbezogenes Datum vorliegt.

Darüber hinaus hat der Bundesgerichtshof in seiner Entscheidung vom 13. Januar 2011 (Az. III ZR 146/10) festgehalten, dass die Befugnis zur Speicherung von IP-Adressen gemäß § 100 Abs. 1 TKG nicht voraussetzt, dass bereits Anhaltspunkte für eine Störung vorliegen. Es genüge vielmehr, dass die Speicherung der IP-Adressen geeignet, erforderlich und verhältnismäßig ist, um abstrakten Gefahren für die Funktionstüchtigkeit des TK-Betriebs entgegenzuwirken.

Sowohl Geeignetheit als auch Erforderlichkeit der Speicherung hat der Gutachter Prof. Martini in seinem Gutachten anschaulich und überzeugend dargestellt.

Die Verhältnismäßigkeit ergibt sich einerseits aus dem Umstand, dass der Kläger die Webseiten der Beklagten freiwillig besucht, er also nicht gezwungen ist, diese Dienste in Anspruch zu nehmen. Nach den Ausführungen des Sachverständigen Dr. Köpsell könnte er, wenn er sich dennoch für eine Nutzung entscheidet, dazu ohne weiteres kostenlos angebotene Anonymisierungsdienste in Anspruch nehmen, die die ihm zugewiesene IP-Adresse unkenntlich machen. Im Übrigen ist die Beklagte, selbst wenn der Kläger keinen Anonymisierungsdienst nutzt, nicht in der Lage, die fragliche IP-Adresse dem Kläger zuzuord-

nen. Dies wäre (jedenfalls was den Anschlussinhaber bzw. das genutzte Endgerät angeht) erst möglich, wenn die Beklagte aufgrund strafprozessualer Ermächtigungen die für die Zuordnung notwendigen Auskünfte vom Provider des Klägers erhalten würde. Soweit entsprechende strafprozessuale Ermächtigungsnormen eingreifen, ist der Kläger insoweit aber nicht mehr schutzwürdig bzw. geht bei entsprechender Güterabwägung das Strafverfolgungsinteresse dem Schutzinteresse des Klägers vor. Anderenfalls würde das Internet zum rechtsfreien Raum, in dem Straftaten nicht mehr verfolgt werden könnten.

Insgesamt liegt somit zwischenzeitlich gefestigte obergerichtliche Rechtsprechung vor, nach der dynamische IP-Adressen gerade keine personenbezogenen Daten darstellen und ihre Speicherung somit zulässig ist.

3.3 Literatur

Die vorgenannte Rechtsprechung hat auch in die datenschutzrechtliche Literatur Eingang gefunden. Auch danach sind IP-Adressen, für die zwar der Provider, nicht aber Dritte mit normalen Mitteln ohne weiteres Zusatzwissen einen Personenbezug herstellen können, keine personenbezogenen Daten (Gola/Schomerus, BDSG, 11. Aufl. 2012, § 3 Rz. 10a; Härting, Internetrecht, 4. Aufl. 2010, Rz. 94). Insoweit hat sich der relative gegenüber dem absoluten Bestimmbarkeitsbegriff in der Literatur weitgehend durchgesetzt (so auch Dammann, in Simitis: BDSG, § 3, Rz. 10).

3.4 Entwicklung des Europarechts

Auch der Verweis des Klägers auf den angeblich europarechtlich herrschenden absoluten Bestimmbarkeitsbegriff vermag nicht zu überzeugen. Unabhängig davon, ob auf europäischer Ebene tatsächlich der absolute Bestimmbarkeitsbegriff führend ist, was ausdrücklich bestritten wird, und unabhängig davon, ob solche europarechtlichen Erwägungen überhaupt Einfluss auf die Entscheidung der hier in Rede stehenden nationalen Rechtsfrage hätten – das OLG Hamburg hat dies ausdrücklich verneint -, zeigen die jüngsten Entwicklungen

der europäischen Gesetzgebung, dass auch auf dieser Ebene der relative Bestimmbarkeitsbegriff eindeutig in die Gesetzgebung einfließen wird.

Im Erwägungsgrund 24 des Entwurfes zur neuen EU-Datenschutz-Grundverordnung vom 22. Juni 2012 ist ausdrücklich festgehalten, dass bei der Nutzung von Online-Services insbesondere auch „identification numbers", also IP-Adressen nicht notwendigerweise personenbezogene Daten darstellen.

Gemäß Art. 4 Abs. 1 des Verordnungsentwurfes handelt es sich bei „personenbezogenen Daten" um Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. „Identifizierbar" ist eine natürliche Person dann, wenn sie durch angemessene Maßnahmen identifiziert werden kann. Gemäß Art. 4 Abs. 1 Satz 2 DS-GVO ist eine natürliche Person dann nicht identifizierbar im Sinne der Verordnung, wenn hierfür ein unverhältnismäßiger („disproportionate") Aufwand an Zeit, Mühe oder sonstigen Mitteln erforderlich wäre. In Fußnote 46 zum Verordnungsentwurf ist weiter ausgeführt, dass insbesondere bei ID-Nummern für Dritte eine Identifizierung nur unverhältnismäßig („disproportionate") möglich wäre.

Damit sind spätestens mit Inkrafttreten der neuen Datenschutzgrundverordnung nicht nur der relative Bestimmbarkeitsbegriff festgeschrieben, sondern darüber hinaus dynamische IP-Adressen für Dritte, also alle außer dem Provider, ausdrücklich von der Definition der „personenbezogenen Daten" ausgenommen.

4. Zusammenfassung

Die Klage ist bereits deshalb unbegründet, da die IP-Adresse des Klägers – auch in Verbindung mit einem Datum und einer Zeitangabe – kein personenbezogenes Datum für die Beklagte darstellt und daher keine Anspruchsgrundlage erkennbar ist, auf deren Basis der Kläger ein Unterlassen der Speicherung von der Beklagten verlangen könnte.

Selbst wenn man die IP-Adresse des Klägers entgegen der obergerichtlichen Rechtsprechung und entgegen weiter Teile der Literatur (in Verbindung mit einem Datum und einer Zeitangabe) als personenbezogenes Datum ansehen würde und deshalb der Kläger grundsätzlich einen Unterlassungsanspruch gemäß §§ 823 Abs. 1, 1004 BGB gegen die Beklagte haben könnte, würde ein Anspruch des Klägers daran scheitern, dass die Rechtsverletzung der Beklagten durch die Speicherung der IP-Adresse bei Abwägung aller Rechtsgüter und Interessen gerechtfertigt und damit nicht rechtswidrig wäre, da die Speicherung für einen sicheren Betrieb der von der Beklagten angebotenen Webseiten unverzichtbar ist. Insoweit müssen die allenfalls abstrakten Datenschutzinteressen des Klägers hinter dem Interesse der Beklagten und allen anderen Nutzern der Webseiten der Beklagten an einem möglichst sicheren Betrieb dieser Webseiten und damit möglichst weitgehendem Schutz vor konkret zu befürchtenden rechtswidrigen Angriffen Dritter zurückstehen.

Wir stellen zu.

[redacted]

Rechtsanwalt

Anlage BB 5

Privat(gegen)gutachten

zur Speicherung von IP-Adressen

Bezug:
Beweisbeschluss des LG Berlin vom 20. Mai 2010
zur Klage gegen die Bundesrepublik Deutschland

Geschäftsnummer 57 S 87/08
2 C 6/08 Amtsgericht Tiergarten

im Rechtsstreit Breyer ./. Bundesrepublik Deutschland

Prof. Dr. Peter Martini

[redacted]

Diplom-Informatiker, Dr.rer.nat.
Universitätsprofessor für Praktische Informatik

Leiter des
Instituts für Informatik IV (Kommunikation und Vernetzte Systeme)
der Universität Bonn
Friedrich-Ebert-Allee 144, 53113 Bonn

Institutsleiter des
Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie,
Fraunhofer-FKIE
Fraunhofer Str. 20, 53343 Wachtberg

Executive Summary

Die Darlegungen des Sachverständigen Dr.-Ing. Stefan Köpsell geben die technischen Sachverhalte beim Betrieb von Webseiten in einer Form wieder, die aus akademischer Sicht als weitgehend korrekt bezeichnet werden kann. Sie ignorieren aber in erheblichem Umfang die gravierenden Sicherheitslücken bei den heute praktisch verfügbaren und im Einsatz befindlichen komplexen IT-Systemen. Erfolgreiche Angriffe von Hacktivisten (wie Anonymous), von Cyber-Kriminellen (wie bei Sony) und von hoch professionellen Angreifern (wie bei den Attacken auf RSA/EMC oder Lockheed Martin) machen deutlich, dass präventive Sicherheit allein nicht ausreichend ist: Umfassende reaktive Maßnahmen sind beim insgesamt beklagenswerten heutigen Stand der Technik zwingend erforderlich, um Sicherheitsvorfälle möglichst frühzeitig zu erkennen, um Sicherheitslücken schnell und zuverlässig zu schließen, um kompromittierte Systeme zu identifizieren und wiederherzustellen. Sie sind auch erforderlich, um die Strafverfolgung und damit die Abschreckung zu unterstützen.

Nur durch Anlage und Pflege umfassender Log-Dateien (inklusive IP-Adressen) kann der Betreiber der Telemedien im Zuständigkeitsbereich des Bundes einerseits seiner Verantwortung für die Betriebssicherheit und -stabilität gerecht werden und andererseits Informationen für Bürger, für unterschiedlichste Organisationen und für öffentliche Einrichtungen bis hin zur kommunalen Ebene auf einem Niveau bereitstellen, wie es bei einem modernen „e-Government" erwartet werden darf bzw. erwartet werden muss.

1. **Dient die Speicherung der IP-Adressen dem nationalen und internationalen Stand der Technik?**
   Die Speicherung der IP-Adressen steht nicht nur, wie Gutachter Köpsell meint, „bestenfalls in Einklang" mit dem Stand der Technik: Sie ist **zwingend erforderlich aufgrund der gravierenden Sicherheitslücken beim heutigen nationalen und internationalen Stand der Technik** im Bereich der IT-Sicherheit. Sie dient insbesondere der technischen Weiterentwicklung von Abwehrmaßnahmen.

2. **Ist eine Speicherung von IP-Adressen nach dem derzeitigen technischen Stand zwingend erforderlich oder bestehen andere Möglichkeiten, um die von der Beklagten betriebenen Webseiten vor schadhaften Angriffen zu schützen oder die Gefahr von Sicherheitsverletzungen zu mindern?**
   Komplexe IT-Systeme müssen heute generell als unsicher gelten, wenn sie dem Nutzer den Komfort bieten, den er vom Internet und den zahlreichen „Apps" gewohnt ist. Die Pflege und die Analyse von Log-Dateien (incl. Speicherung von IP-Adressen) ist eine (von mehreren) wertvollen Maßnahmen zum Schutz von IT-Systemen, zur Erkennung von Sicherheitsvorfällen, zur Verkürzung von Reaktionszeiten und zur gezielten Warnung potentiell Geschädigter. Sie kann NICHT durch andere Maßnahmen ersetzt werden.

3. **Welche Kosten wären gegebenenfalls für andere Maßnahmen aufzuwenden?**
   Die Speicherung von IP-Adressen kann NICHT durch andere Maßnahmen kompensiert werden: Sie muss durch andere Maßnahmen ergänzt werden.

Detaillierte gutachterliche Stellungnahme

Einleitende Anmerkungen:

Das Bundesamt für Sicherheit in der Informationstechnik, BSI, hat mich mit Schreiben vom 3. September 2012 beauftragt, als Sachverständiger ein Privatgutachten zu erstellen, das sich am Beweisbeschluss des LG Berlin vom 20. Mai 2010 orientiert und zu der Frage Stellung nimmt, ob die Speicherung und spätere Verwendung von IP-Adressen der zugreifenden Hostsysteme durch die Beklagte erforderlich ist, um die IT-Sicherheit und die Funktionsfähigkeit der von ihr betriebenen und verwendeten Telemedien und Telekommunikationsnetze zu gewährleisten und aufrecht zu erhalten.

Der hier in Frage stehende Sachverhalt betrifft Kernfragen, mit denen ich mich in meiner beruflichen Tätigkeit als Leiter des Instituts für Informatik IV der Universität Bonn seit vielen Jahren in Forschung und Lehre befasse und zu denen ich als Leiter des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie, FKIE, besondere Verantwortung trage: FKIE ist ein Institut, das sich unter meiner Leitung mit derzeit ca. 370 Mitarbeiterinnen und Mitarbeitern fast ausschließlich mit Fragen der Verteidigung und der Sicherheit befasst. Nachdem ich im Sommer 2010 die Leitung von FKIE übernommen habe, konnte ich die Aktivitäten im Bereich der präventiven IT-Sicherheit, der reaktiven IT-Sicherheit sowie der Analyse von Schad-Software (sog. „Malware") und der Abwehr von Botnetzen stark ausbauen , so dass bei FKIE heute ca. 50 Mitarbeiterinnen und Mitarbeiter im Bereich der „Cyber-Defense" bzw. der „Cyber-Security" tätig sind. Wie bei einem Fraunhofer-Institut kaum anders zu erwarten, liegt der Schwerpunkt der Aktivitäten im Bereich der anwendungs-orientierten Forschung bzw. des Technologie-Transfers und der Überbrückung der Lücke zwischen der wissenschaftlich erarbeiteten Theorie und der Praxis der in der Realität eingesetzten Systeme.

Bekanntlich ist der Unterschied zwischen Theorie und Praxis in der Praxis noch größer als in der Theorie. Dies gilt in besonderer Weise für die Theorie und die Praxis der heute im Einsatz befindlichen IT-Systeme und damit für die hier zu beantwortende Frage nach der zwingenden Notwendigkeit der Speicherung von IP-Adressen: Aus Sicht der Theorie lassen sich sichere IT-Systeme realisieren. In der Praxis erweist sich dagegen schon die Bereitstellung attraktiver Web-Angebote als unerwartet komplex und fehleranfällig.

1. Grundlegende Betrachtung zum Betrieb öffentlicher Internetportale

Die nachfolgende Betrachtung beschreibt in möglichst allgemein verständlicher Form, auf welche Weise nach dem heutigen Stand der Technik ein öffentlich wirksames Online-Angebot im World Wide Web betrieben wird. Hierbei fokussiert die Darstellung auf das Zusammenspiel der wichtigsten Komponenten und deren Einbindung in die Sicherheitsarchitektur des IT-Systems des Diensteerbringers.

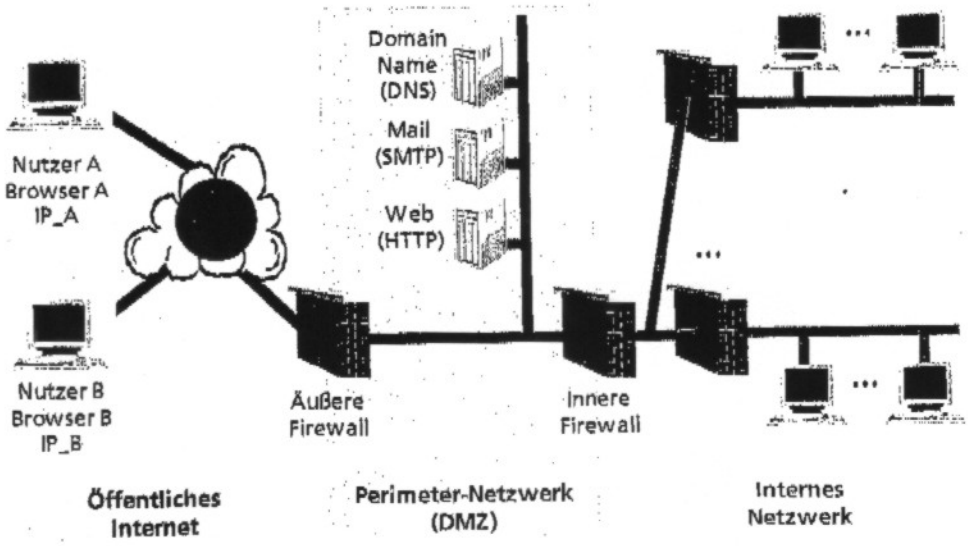

Abbildung 1: Web-Server im Perimeter-Netzwerk (DMZ: Demilitarized Zone)

Die eigentlichen Inhalte werden bei größeren Web-Präsenzen im Regelfall in einem **„Content-Management-System" (CMS)** verwaltet, das insbesondere für eine effiziente Speicherung und Bereitstellung sowie für die Konsistenz der angebotenen Informationen sorgt. Weite Verbreitung haben etwa das Open-Source-CMS „Plone" mit dem zugehörigen Web-Framework „Zope" und das Content-Management-System der Firma CoreMedia AG.

Die Bereitstellung der vom CMS generierten Information erfolgt nicht über das CMS direkt, sondern über **Web-Server**, die Zugang zum Internet haben und es den Client-Programmen (Web-Browser wie etwa Firefox, Chrome, Internet Explorer, Opera, ...) ermöglichen, gemäß einem standardisierten Ablauf (dem HTTP-Protokoll) speziell formatierte Dokumente (HTML) mit Hinweisen auf den Ort der Lagerung weiterer Daten abzurufen. Neben der klassischen textuellen Darstellung mit Einbindung einfacher Graphiken beinhalten moderne Web-Seiten häufig auch „aktive Inhalte", insbesondere Videos als „Flash-Movies" und „Java-Applets". Letztere ermöglichen es dem Betreiber von Web-Seiten, Programme bereit zu stellen, die an die Client-Systeme der Web-Nutzer übertragen und dort in einer „Sandbox" (mit stark eingeschränkten Zugriffsrechten auf die lokale Systemumgebung) ausgeführt werden. Dies geschieht unter anderem, um etwa komplexe Sachverhalte zu veranschaulichen und hierbei Interaktion mit dem Benutzer durch Eingabe von alphanumerischen Zeichen oder durch Nutzung von „Buttons" oder „Check Boxes" zu ermöglichen. Theoretisch ist der Betrieb von Java-Applets in einer Sandbox des Client-Systems sicher; in der Praxis gilt dies leider nicht immer.

Web-Server sind nicht unmittelbar lauffähig: Sie benötigen eine **Betriebssystem-Umgebung**, wie sie etwa durch Linux oder durch Windows bereitgestellt wird. Der bereits erwähnte Apache-Server wurde ursprünglich für Linux entwickelt, ist aber auch für andere Betriebssysteme wie etwa Windows verfügbar.

2. Angriffe auf öffentliche Internetportale bzw. über diese hinweg

Angriffe auf Internetportale können sich nicht nur gegen den eigentlichen Web-Server richten, sondern auch gegen dessen Systemumgebung: Aufgrund der Internet-weiten Sichtbarkeit und der Internet-weiten Erreichbarkeit können Web-Server leicht als Ziele identifiziert werden. Darüber hinaus dienen Angriffe auf Web-Server häufig dazu, Schad-Code einzuspielen und dort zu speichern, um die Client-Systeme der Nutzer zu kompromittieren, wenn sie auf derart infizierte Web-Seiten zugreifen. Nutzer sind insbesondere durch „Drive-by Infektionen" gefährdet, wenn ein Angreifer Zugriff auf Web-Server oder Content-Management-Systeme erlangt. Beim aktuellen Stand der Technik kann auch bei größter Sorgfalt des Betreibers leider nicht aus ausgeschlossen werden, dass Unbefugte Zugang erlangen und gezielt Schad-Software auf den Web-Server bringen, um Sicherheitslücken in Client-Systemen zu nutzen und Zugriff auf diese zu erlangen, d.h. die Client-Systeme zu „hijacken". In der Tat ist das Risiko für derartige Attacken, die über längere Zeit erfolgreich sein und unerkannt bleiben können, mittlerweise so groß, dass aus meiner Sicht die Log-Dateien der IT-Systeme des Bundes regelmäßig und mit immer besseren Methoden auf Hinweise zu erfolgreichen Angriffen überprüft werden müssen.

2.1. Angriffe auf Web-Server

„Unfortunately, Web Servers are often the most targeted and attacked hosts on organization's networks". Mit diesen Worten beginnt die inhaltliche Darstellung der Executive Summary zu den "Guidelines on Securing Public Web Servers", die das NIST (National Institute of Standards and Technology) als "Special Publication 800-44, Version 2" im September 2007 veröffentlicht hat, vgl. [NIST 2007].

Die Situation hat sich seither noch massiv verschärft, denn heute führen „Cyber-kriminelle" in großem Umfang Attacken durch, bei denen Software-Tools zum Einsatz kommen, die es gestatten, Tausende Webseiten effizient auf Sicherheitsrisiken zu überprüfen und identifizierte Schwachstellen konsequent zu nutzen. Es ist nicht übertrieben zu sagen, dass es heute in normalen Wohngebieten in Deutschland sehr viel sicherer ist, die Haustüre über Nacht unverschlossen zu lassen, als einen Web-Server nur wenige Minuten oder gar wenige Stunden ungeschützt zu lassen. Insbesondere muss davon ausgegangen werden, dass Sicherheitslücken unmittelbar nach Bekanntwerden so schnell und so konsequent von professionellen Angreifern genutzt werden, dass den Betreibern von Web-Servern nur wenig Zeit bleibt, um ihre Systeme zu sichern. Noch kritischer sind die „Zero-Days": Vorhandene, aber bislang nicht

identifizierte Sicherheitslücken, die gewissermaßen zum „Tag Null" des Problembewusstseins für Angriffe genutzt werden.

Als aktuelles Beispiel für den Umgang mit bekannten Sicherheitslücken seien hier Schwachstellen im weit verbreiteten Content-Management-System „Plone" genannt: Am 1. November 2012 warnte Plone vor schwerwiegenden Sicherheitslücken in der von Plone bereit gestellten Software, vgl. [PLONE 2012]. Details zu diesen Sicherheitslücken waren in gewissen Kreisen war offensichtlich bekannt, doch wurden nähere Angaben zur Art der Schwachstellen aus Sicherheitsgründen nicht gemacht. Ein „Patch" zum Schließen der Lücken wurde angekündigt für den 16. November 2012, 15:00 UTC (Coordinated Universal Time). Mit dieser Vorankündigung erging die Empfehlung an alle Betreiber, für die 60 Minuten nach Bereitstellung des Patches ein Wartungsfenster einzuplanen, um die Sicherheitslücken unmittelbar nach Bekanntwerden zu schließen. In der Zwischenzeit – immerhin ca. 2 Wochen – waren die Systeme offen für Angreifer, denen diese kritischen Lücken und die Art der Nutzung bekannt waren. Dieses durchaus beunruhigende Szenario ist zudem noch als positiver Fall zu werten: Nur selten gibt es derart rechtzeitige Vorankündigungen mit konkreter Handlungsempfehlung.

In ihrer weithin beachteten grundlegenden Arbeit [KOSS 2000] haben Kossakowski und Allen bereits im Jahr 2000 die drei sicherheitsrelevanten Bereiche charakterisiert, die beim Betrieb von öffentlichen Web-Portalen zu beachten sind:

a) Denial-of-Service-Attacken
b) Kompromittierung des Web-Servers
c) Angriffe über die unterlagerte Systemumgebung

2.1.1. Denial-of-Service-Attacken

Die Denial-of-Service-Attacken verfolgen das Ziel, die Verfügbarkeit der vom Web-Server angebotenen Dienste einzuschränken oder auch völlig zum Erliegen zu bringen, um legitime Nutzer, also Menschen oder Computer-Programme auf anderen Systemen, in ihrer Tätigkeit bzw. Funktionsweise zu behindern.
Bei einer Denial-of-Service-Attacke werden im Regelfall mit Schad-Software infizierte Systeme dazu veranlasst, Datenpakete an das angegriffene System zu senden. Können hinreichend viele infizierte Systemen über eine Kommando-und-Kontroll-Struktur gesteuert und zu (im Regelfall fast beliebigen) Aktionen veranlasst werden, spricht man von „Botnetzen", bei denen die infizierten Computer wie „Roboter" (kurz: Bot) ferngesteuert werden. Als Beispiel für derartige Botnetze, von denen es heute Tausende gibt, sei MINER genannt: MINER wurde im Jahr 2011 für Angriffe auf bekannte deutsche Web-Portale genutzt, u.a. für Angriffe auf Immobilienscout24 und Pizza.de. In einigen extremen Fällen der jüngeren Vergangenheit wurden die angegriffenen Systeme auf die hier skizzierte Weise mit einer Last von bis zu mehreren Hundert Gigabit/Sekunde geflutet, so dass nicht nur der angegriffene Web-Server überlastet wurde, sondern auch die Datenleitungen dorthin. Die Abwehr derartiger Attacken kann nur durch den Internet Service Provider erfolgen, der hierzu aber

Kenntnisse über die Art des Angriffs braucht, um entsprechende Datenpakete blockieren zu können.
Eine andere Variante von Denial-of-Service-Attacken besteht darin, Sicherheitslücken im Web-Server zu nutzen und durch speziell geformte Anfragen dafür zu sorgen, dass der Web-Server handlungsunfähig wird. Als Beispiel sei eine kritische Sicherheitslücke im Apache-Web-Server genannt, über die im August 2011 berichtet wurde und bei der es möglich ist, von nur einem Angriffs-Rechner aus Anfragen zu senden, mit denen der Speicher des Web-Servers überlastet wird, was den Server funktionsunfähig macht , vgl. [HEISE 2011].

Die Speicherung von IP-Adressen ist ein unverzichtbares Hilfsmittel, um Denial-of-Service-Attacken analysieren und erfolgreich abwehren zu können.

2.1.2. Kompromittierung des Web-Servers

Eine Kompromittierung des Web-Servers verfolgt häufig das Ziel, sensible Informationen zu gewinnen und ggf. auch zu verändern. Zu dieser Art von Angriffen gehört etwa der Zugriff auf Informationen, die zwar auf dem Web-Server gespeichert sind, die aktuell aber nicht, noch nicht oder nicht mehr öffentlich verfügbar sein sollen. Beim sog. „Defacement", also bei der Verunstaltung von Webseiten, wird der Server so manipuliert, dass (im Regelfall hochgradig unerwünschte) Darstellungen entstehen, um den Betreiber bloß zu stellen. Ein völlig anderes Ziel kann darin bestehen, Informationen über Nutzer und Administratoren von Web-Servern zu gewinnen, insbes. deren Passwörter auszuspionieren. Es kann auch das Ziel verfolgt werden, Informationen über die Konfiguration des Web-Servers und/oder der angeschlossenen Netz- und Systemumgebung zu gewinnen, um diese Kenntnisse bei nachfolgenden Attacken zu nutzen. Auf die hier skizzierte Art kann ein professioneller Angreifer den Versuch unternehmen, den kompromittierten Web-Server als „stepping stone" zu missbrauchen für eine Attacke auf andere Computer-Systeme beim Betreiber des Web-Servers, für eine Attacke auf andere Nutzer des Web-Servers und auch für eine Attacke auf Organisationen mit besonderer Vertrauensbeziehung zum Betreiber des Web-Servers. Insbesondere dient der Web-Server dann also als Werkzeug bzw. als Sprungbrett für tiefergehende Attacken. Dies gilt insbesondere dann, wenn der Web-Server dynamisch durch sog. **„Backend-Server"** mit den vom Web-Client gewünschten Informationen versorgt wird. Bei Sicherheitslücken kann es dem Angreifer hier gelingen, den Backend-Server zu kompromittieren und über diesen hinweg weitere Systeme des Betreibers anzugreifen.

Beim klassischen Web-Angebot erfolgt die Bearbeitung und Bereitstellung der Inhalte für das Web durch wenige Personen, die im Regelfall beim Betreiber oder im Auftrag des Betreibers tätig sind. Beim „Web 2.0" verlässt der Nutzer hingegen die Rolle des reinen Konsumenten mit ggf. weit reichenden Möglichkeiten der Recherche: Bei Web 2.0 wird der Nutzer über das Client-System zum aktiven Gestalter von Inhalten auf dem

Server-System. Diese tiefere Interaktion maximiert zwar die „User Experience", steigert aber auch die Risiken für Sicherheitsvorfälle erheblich.

Das Technical White Paper „2011 Top Cyber Security Risks Report", [HP 2011], charakterisiert Web-Anwendungen als "significant risk to the enterprise": Mehr als ein Drittel der insgesamt im Jahr 2011 bekannten Sicherheitslücken wird in diesem Report dem Bereich der „Web-Anwendungen" zugeordnet. Die Zahl der bekannten Verwundbarkeiten ist zwar von 6000 im Jahr 2006 auf ca. 2000 im Jahr 2011 gesunken, doch muss bei einer derart hohen Zahl immer noch eher von Unsicherheit gesprochen werden als von Sicherheit. Schlimmer noch: Die genannte Zahl beschreibt nur die bekannten Verwundbarkeiten.
Der Report von Hewlett-Packard beschreibt auch Ergebnisse, die bei der Suche nach Sicherheitslücken in Web 2.0 – Anwendungen erzielt wurden: Obwohl nur 22 % der betrachteten Systeme Dienste anbieten, die mit dem Schlagwort Web 2.0 bezeichnet werden, wurden etwa 50 % der insgesamt entdeckten kritischen Sicherheitslücken in Web 2.0 – Systemen gefunden.
Zweifel daran, ob die von Hewlett-Packard präsentierten Ergebnisse repräsentativ sind und – wenn ja – ob diese Ergebnisse sich auf Web-Präsentationen von Ministerien und Behörden der Bundesrepublik Deutschland übertragen lassen, sind durchaus angebracht. Festzuhalten bleibt jedoch, dass sehr viele der heutigen attraktiven Web-Präsenzen erhebliche Sicherheitslücken aufweisen und dass diese wesentlich im komplexen Zusammenspiel von jeweils in sich schon komplexen Software-Modulen begründet sind.
Viele der heute bei Internetportalen eingesetzten Software-Pakete wurden aus der Erkenntnis heraus entwickelt, dass Einzelkämpfertum bei der Programmierung von Web-Präsenzen nicht zielführend ist, wenn all das an Funktionalität und Konsistenz gewünscht wird, was in der Breite des Internet heute State-of-the-Art ist: Handgestrickte Lösungen sind nicht zielführend, wenn der angestrebte Web-Auftritt den staatlichen Institutionen der Bundesrepublik Deutschland angemessen sein soll. Dennoch bleibt zu beachten, dass bei Einsatz der gängigen Software-Lösungen auch deren Schwachstellen und die damit verbundenen Risiken übernommen werden.

Die Speicherung von IP-Adressen ist ein unverzichtbares Hilfsmittel, um erfolgreiche Angriffe auf Web-Server analysieren zu können. Diese Analysen dienen der Schadensidentifikation und –begrenzung; sie dienen auch der Weiterentwicklung von präventiven Maßnahmen.

2.1.3. Angriffe auf die unterlagerte Systemumgebung

Ein erfolgreicher Angriff auf die unterlagerte Systemumgebung kann es dem Angreifer ermöglichen, die Software des Web-Servers gewissermaßen zu unterwandern und die Kontrolle nicht nur über den eigentlichen Web-Server, sondern gleich auch über das gesamte „Host-System" zu übernehmen. Als „Host" wird hier das Computer-System bezeichnet, auf dem der Web-Server als Software installiert ist. Die Software des Web-Servers ist gewissermaßen auf dem Host-System gekapselt: Das gesamte Verhalten wird

vom Betriebssystem aktiv unterstützt und auch überwacht. Insbesondere läuft die gesamte Kommunikation mit dem Client-System und mit den weiteren Servern, aus denen Daten für den Web-Server bereitgestellt werden, über entsprechende Mechanismen des Betriebssystems auf dem Host.

Da bei allen gängigen Betriebssystemen immer wieder Sicherheitslücken gefunden werden, müssen diese im Rahmen eines zeitnahen Patch-Managements durchgängig geschlossen werden. Leider gab es in jüngerer Vergangenheit schwerwiegende Sicherheitsvorfälle gerade bei derartigen Updates bzw. durch Missbrauch der Update-Funktionalität: Erst in der ersten Jahreshälfte 2012 wurde erkannt, dass die offenbar bereits im Jahr 2008 entwickelte Schad-Software „Flame" den Windows-Update-Mechanismus nutzt, um diese ungewöhnlich große Schad-Software als Windows Update zu tarnen – unter Ausnutzung einer kryptographischen Attacke gegen die im Internet weit verbreitete Signatur mittels „MD5": Microsoft hatte zwar aufgrund der zwischenzeitlich erkannten Schwächen im Dezember 2008 davor gewarnt, MD5 für die Unterzeichnung von digitalen Zertifikaten zu nutzen, hatte aber versäumt, MD5 in den relevanten Teilen der eigenen Betriebssysteme zu ersetzen. Auch Windows 7 war nicht geschützt. Somit kann es nicht verwundern, dass nach Angaben der Antiviren-Industrie etwa die Hälfte der bekannt gewordenen Infektionen durch Flame das Betriebssystem Windows 7 betrifft.

Angriffe auf das unterlagerte Betriebssystem und damit auf die unterlagerte Systemumgebung haben für die in diesem Gutachten behandelten Fragen besondere Relevanz, weil Web-Services (und ähnliche öffentliche Internetportale) die ihnen unterlagerten Computer internetweit sichtbar und damit auch angreifbar machen: Auch die entlegensten Bereiche von öffentlichen Web-Auftritten sind mit entsprechenden Mechanismen suchbar und identifizierbar. Bei komplexen Internet-Auftritten, die im Zusammenspiel verschiedener Computer erbracht werden, wird der Angreifer bei professionalisierten Attacken gezielt nach angreifbaren Teil-Systemen suchen und diese kompromittieren.

2.2. Angriffe auf Client-Systeme

Die europäische Netzsicherheitsagentur ENISA warnte am 5. Juli 2012 in einer Pressemitteilung: „Davon ausgehen, dass alle PCs infiziert sind" [ENISA 2012]. Diese Empfehlung richtete sich an Banken, denen in der aktuellen Situation nahegelegt wurde, bei ihren Schutzmaßnahmen davon auszugehen, dass die PCs der Nutzer mit Schad-Software infiziert seien – insbesondere durch die Schad-Software „Zeus", die seit 2007 als Standard-Virus bekannt ist und für die Do-it-Yourself-Virus-Kits schon für etwa 1000 Euro erhältlich sind.

Die zahlreichen spekulativen Berichte über den Grad der Verseuchung von PCs mit Schad-Software sollen hier nicht zitiert werden. Stattdessen seien hier einige belastbare Zahlen aus dem Bericht der Deutschen Telekom „Sicherheit im Internet, August 2012" genannt: Dem Bericht ist zu entnehmen, dass die Deutsche Telekom im ersten Halbjahr 2012 insgesamt 137.237 Kunden darüber informiert hat, dass ihr Rechner vermutlich mit Schad-Software infiziert ist, vgl. [DTAG 2012]. Anlass hierzu gaben ca. 7 Millionen Hinweise auf Missbrauch von Diensten der Deutschen Telekom, die im ersten Halbjahr 2012 bei diesem Internet Service Provider eingingen.

Eine großer Anteil der Neu-Infektionen von PCs und Laptops geht heute auf sog. „Drive-By Infections" zurück, also auf „Infektionen im Vorbeifahren": Für eine Infektion ist es schon ausreichend, zu einer Web-Seite zu surfen, die von einem Angreifer systematisch manipuliert wurde, ohne dass der Betreiber der Web-Seite dies bemerkt hat. Der Besucher einer derart infizierten Seite muss also selbst keine Downloads starten oder Installationen vornehmen – das übernimmt die infizierte Web-Seite automatisch ohne Zutun des Nutzers. Da diese Art der Infektion die normalen Wege des Surfens im Web nutzt, bieten Firewalls und auch Adress-Umsetzungen (NAT – Network Address Translation) dem Client-System keinerlei Schutz.

Wesentlich erleichtert wird die starke Zunahme von Drive-By Infections dadurch, dass immer mehr Web-Seiten aktive / dynamische Inhalte integrieren und hierzu Technologien wie JavaScript, Java, Adobe Flash, ActiveX oder PHP einsetzen. Hierbei wird ausführungsfähiger Programm-Code an das Client-System übertragen, wo dieser Programm-Code in einer Komponente des Browsers läuft, die meist als „Sandbox" bezeichnet wird. Eine derartige Sandbox soll sicherstellen, dass das vom Web-Server übermittelte Programm nur in einem abgegrenzten Bereich laufen kann und keinen allgemeinen Zugriff auf den Client-Computer hat.

Leider gab und gibt es immer wieder Fälle hochgradig kritischer Sicherheitslücken in Browsern und in Sandboxen. Populärstes Beispiel der jüngeren Vergangenheit ist wohl die Schwachstelle in der aktuellen Version von Java, vor der im August 2012 gewarnt wurde, vgl. [BSI 2012]. Da es zunächst kein Patch gab, wurde empfohlen, das Java-Plug-In für die gängigen Browser zu deaktivieren. Eine derartige Deaktivierung bedeutet aber, dass auf viele Web-Seiten gar nicht mehr zugegriffen werden kann, weil der Zugriff Java voraussetzt.

2.3. Zielgerichtete Angriffe (Advanced Persistent Threats, APTs)

Bei den sog. „Advanced Persistent Threats" handelt es sich um eine neue Art von hoch professionellen und zielgerichteten Attacken, deren Bedeutung in jüngerer Vergangenheit deutlich zugenommen hat. Bekannte Beispiele sind Stuxnet, Duqu, Flame und Aurora.

Advanced ... sind diese Attacken, weil sie mit sehr großem Aufwand vorbereitet werden: Relevante Informationen werden vorsichtig und in der Regel unbemerkt ausgespäht, hoch spezialisierte Schad-Software wird für ein ganz bestimmtes Zielsystem oder für eine Klasse von Zielsystemen professionell erstellt.

Persistent ... werden diese Angriffe dadurch, dass der Angreifer „niedrig hängende Früchte" wie opportunistische Informationssuche oder schnellen finanziellen Gewinn vermeidet und stattdessen ein vorrangiges Ziel konsequent verfolgt. Zentral ist neben einem häufig gewünschten Durchdringen zu bestimmten, gut geschützten Zielsystemen meist der Wunsch, langfristig Zugang zum kompromittierten System zu halten und hierbei unentdeckt zu bleiben.

Threats ... also Bedrohungen besonderer Art entstehen primär dadurch, dass hier hohe technische Fähigkeiten mit konsequentem, zielorientiertem Handeln verbunden werden, um ein ganz bestimmtes Ziel zu erreichen.

Typischerweise werden bei APTs nicht nur IT-Systeme in Mitleidenschaft gezogen, die direkt mit dem Angriffsziel in Zusammenhang stehen, sondern es werden IT-Systeme als Zwischensysteme missbraucht.

Aufgrund der spezifischen Charakteristika von APTs, wie sie exemplarisch im Kontext Stuxnet einer breiteren Öffentlichkeit bekannt geworden sind, ist es offensichtlich, dass die IT-Systeme öffentlicher Einrichtungen in besonderer Weise bedroht sind.

2.4. Angreifbarkeit von „gut gesicherten Systemen"

Die Ausführungen in den vorangegangenen Teilkapiteln haben bereits deutlich gemacht, dass auch bei „gut gesicherten Web-Servern" kein Sicherheitsniveau erreichbar ist, das ohne reaktive Maßnahmen für die Belange der Ministerien, Ämter und sonstigen Behörden des Bundes ausreichend ist: Ein wirklich gut gesichertes Haus ist ein Haus, bei dem Türen und Fenster zugemauert wurden, denn auch für die neuesten Schlösser finden sich Profis, die in der Lage sind, ohne Schlüssel ins Haus einzudringen. Da ein solches Haus für die Bewohner nicht akzeptabel ist, gibt es Alarmanlagen und Wachdienste.

Auch gut gesicherte Web-Server sind in einem Umfang verwundbar, der ohne zusätzliche Sicherungssysteme durch Monitoring und konsequente Prüfung von Log-Dateien für die hier relevanten Anwendungen nicht akzeptabel ist.

Anzumerken ist hier noch, dass insbesondere bei Advanced Persistent Threats das Risiko durch Innentäter nicht vernachlässigt werden darf, denn APTs setzen insbesondere auch „Social Engineering" ein. So werden etwa ausgewählte Mitarbeiter gezielt auf infizierte Web-Seiten gelockt, um Mitarbeiter-Computer zu infizieren und auf diesem Wege mit den Rechten der Mitarbeiter das Netz erkunden zu können.

Wo Menschen an komplexen Systemen arbeiten, da werden auch Fehler gemacht, die nach Möglichkeit (aber nicht immer) zeitnah erkannt werden und behoben werden müssen. Weiterhin können Mängel in der Regelung von Zuständigkeiten leicht dazu führen, dass Web-Server (wie auch andere IT-Systeme) in nicht akzeptabler Weise verwundbar sind.

Auch bei Systemen, die durch präventive Maßnahmen gut oder vermeintlich gut gesichert wurden, kann somit auf reaktive Maßnahmen nicht verzichtet werden: Kompromittierungen müssen in sicherheitsrelevanten Bereichen durch geeignete Systemüberprüfungen so früh wie möglich erkannt und beseitigt werden.

3. Sicherer Betrieb von Internetportalen

Die nachfolgenden Betrachtungen diskutieren zunächst Gemeinsamkeiten und Unterschiede bei der Absicherung von Computer-Systemen im Vergleich zur Absicherung von Werten in der realen Welt. Hierbei wird deutlich, dass angesichts der Bedrohungslage und des heutigen Stands der Technik rein präventive Maßnahmen nicht ausreichend sind, um öffentliche Internetportale staatlicher Einrichtungen hinreichend zu schützen: Zusätzlich – also NICHT alternativ – sind reaktive Maßnahmen erforderlich. Die Diskussion in Abschnitt 3.3. zeigt, dass hierbei auf IP-Adressen im Klartextformat nicht verzichtet werden kann.

3.1. Grundsätzliches zur Absicherung von realen und digitalen Werten

Im Folgenden werden zunächst grundsätzliche Betrachtungen zur Absicherung von Werten angestellt. Für eine weitergehende Diskussion sei beispielsweise auf [BISKUP2009] sowie weitere Lehrbücher verwiesen.

Sowohl in der digitalen als auch in der realen Welt basiert der erfolgreiche Einsatz von Sicherheitsmaßnahmen auf zahlreichen Annahmen, die in der Praxis sehr schwer zu erfüllen sind. Hinsichtlich der Absicherung eines Wohnhauses in der realen Welt gehören zu diesen Annahmen beispielsweise die folgenden:

- Die Türe ist die einzige Zutrittsmöglichkeit zum Haus. Es kann beispielsweise nicht durch die Fenster betreten werden.
- Die Hersteller, Lieferanten und Verkäufer der Türen, Schlösser und Schlüssel agieren regelkonform und missbrauchen nicht das in sie gesetzte Vertrauen; keine dieser Parteien behält Duplikate der Schlüssel.
- Die Hausbewohner verlieren keine Schlüssel.
- Es gibt keine Gelegenheit für nicht vertrauenswürdige Personen, Schlüsselkopien zu erstellen.
- Wenn die Hausbewohner für den Notfall einen Schlüssel den Nachbarn anvertrauen, dann werden die Nachbarn nur im Interesse der Hausbewohner mit diesem Schlüssel tätig.
- Einbrecher werden entweder durch die Schutzmaßnahmen abgeschreckt oder scheitern daran, die Türe aufzubrechen.

Aufgrund der Schwierigkeiten, diesen Annahmen in der Praxis in vollem Umfang gerecht zu werden, muss die Möglichkeit des Versagens der Schutzmaßnahmen in Betracht gezogen werden. Es werden daher zusätzliche reaktive Schutzmaßnahmen ergriffen, z.B. die Installation einer Alarmanlage und/oder die Beauftragung eines Wachdienstes.

Bei hohen, schutzwürdigen Werten ist die dargestellte Absicherung der Außengrenzen des Wohnhauses für die Sicherheit insgesamt nicht ausreichend. Auch im Inneren des Hauses müssen Sicherheitsmaßnahmen ergriffen werden. Beispielsweise werden auch die Zimmertüren mit Schlössern versehen, Wertgegenstände in verschlossenen Stahlschränken aufbewahrt und darüber hinaus Bewegungsmelder im Inneren eines Hauses installiert und mit der Alarmanlage gekoppelt, wenn hohe Werte zu schützen sind.

Die dargestellten Betrachtungen berücksichtigen allein die Perspektive und die Interessen der Hausbewohner bzw. –eigentümer. Im Allgemeinen sind jedoch weitere Parteien involviert wie z.B. Besucher, Nachbarn, die finanzierende Bank, Versicherungen, der Wachdienst und andere.

Deutlich wird, dass in der realen Welt präventive und reaktive Sicherheitsmaßnahmen ergänzend zueinander eingesetzt werden, um ein angemessenes Maß an Sicherheit zu erreichen.

In der digitalen Welt werden zur Absicherung von IT-Systemen präventive Sicherheitsmaßnahmen wie Zugangs- und Zugriffskontrollsysteme eingesetzt. Sie dienen dazu, alle in der sog. „Security Policy" erlaubten bzw. untersagten Zugriffe entsprechend zu gewähren oder zu verweigern. Dem liegen folgende Annahmen zugrunde:

- Die Security Policy spezifiziert **exakt** die gewünschten erlaubten Zugriffe bzw. untersagten Zugriffe.
- Die Verantwortlichen beschreiben die Security Policy **korrekt** und **vollständig**.
- Die Security Policy kann im IT-System **vollständig** repräsentiert werden.
- Die Zugangs- und Zugriffskontrollsysteme können nicht umgangen werden und sie setzen die Security Policy ohne Ausnahme durch.

Leider sind diese Annahmen in der Praxis schwer oder teils unmöglich zu erfüllen, so dass der reale Betrieb von IT-Systemen typischerweise durch folgende Situationen gekennzeichnet ist:

- Die Security Policy ist im mathematisch/formalen Sinne unpräzise und unvollständig. Zentrale Bedeutung hat hier, dass Kontextinformation nur begrenzt berücksichtigt werden kann.
- Die Sprachen zur Beschreibung von Security Policyen sind nicht ausdrucksstark genug, so dass die Security Policy nicht exakt repräsentiert werden kann. Beispielsweise kann oftmals nicht zwischen der Ergänzung und der Modifikation von Dokumenten unterschieden werden: Anstatt Zugriffe auf Ergänzungen zu beschränken, müssen pauschal Modifikationen erlaubt werden, um das IT-System benutzbar zu halten.
- Die Zugriffskontrollkomponenten zur Durchsetzung der Sicherpolitik betrachten nicht alle Zugriffsanforderungen.

- Administratoren oder Benutzer deaktivieren einzelne Zugriffskontrollmechanismen aus Effizienz- oder Komfortgründen.
- Angreifer finden Wege, um die Zugriffskontrolle zu umgehen oder zu deaktivieren.

Die Ursachen für diese Situationen liegen nur teilweise in dem achtlosen oder bösartigen Verhalten der verschiedenen Personen, die an der Konstruktion und dem Betrieb sicherer IT-Systeme beteiligt sind. Vielmehr existieren inhärente Schwierigkeiten, ein wirklich hohes Maß an Sicherheit zu erreichen. Beispiele für bestehende Unzulänglichkeiten sind die folgenden:

- Im Allgemeinen ist die Umsetzung der Zugriffskontrollanforderungen auf Computern schwer zu handhaben, worauf Unentscheidbarkeitsresultate in wissenschaftlichen Arbeiten beispielsweise im Bereich der Informationsflusskontrolle hindeuten.
- Aus Effizienzgründen können Zugriffskontrollanforderungen nur grob durch Zugriffsrechte approximiert werden.
- Ein Benutzer kann für seine legitimen Pflichten eine Menge spezifischer Zugriffsrechte benötigen, jedoch stellen nicht alle Kombinationen der Nutzung dieser Zugriffsrechte akzeptables Verhalten dar.

Auch in der digitalen Welt sind präventive Sicherheitsmechanismen diversen Unzulänglichkeiten, Schwierigkeiten und der Imperfektion der Realität unterworfen, so dass ein Versagen der Schutzmechanismen einzukalkulieren und entsprechende Vorsorge durch zusätzliche nämlich reaktive Schutzmechanismen zu treffen ist. Die naheliegende Erweiterung der Zugriffskontrolle um Zugriffsprotokollierung (Logging/Monitoring) liefert hierfür die Basis:

- Alle Zugriffsanfragen werden protokolliert und für einen angemessenen Zeitraum gespeichert.
- In Ergänzung der Beurteilung einzelner Zugriffsanfragen durch die Zugriffskontrolle können die protokollierten Daten (gewissermaßen nachträglich) hinsichtlich (komplexer) **Sequenzen von Zugriffsanfragen** analysiert werden. Zielsetzung dieser Analysen sind die Suche nach Angriffen, also die Suche nach Mustern von charakteristischem, unerwünschtem Verhalten, und eine entsprechende Reaktion auf erkannte Angriffe.

Offensichtlich können sowohl in der realen als auch in der digitalen Welt weder präventive noch reaktive Sicherheitsmechanismen perfekten Schutz sicherstellen. Vielmehr verringert der komplementäre Einsatz von präventiven und reaktiven Sicherheitsmechanismen die Lücken, die ausschließlich präventive Sicherheitsmechanismen hinterlassen.

Neben vielen grundsätzlichen Gemeinsamkeiten bei der Absicherung von digitalen und realen Werten existieren auch signifikante Unterschiede.

In der digitalen Welt ist das Risiko für einen Täter, ertappt und zur Verantwortung gezogen zu werden, um ein Vielfaches geringer als in der realen Welt. Die erforderlichen Kenntnisse und Fähigkeiten zur Durchführung von Einbrüchen und Angriffen sind in der digitalen Welt einfach kopierbar und vervielfältigbar. Insbesondere können Abläufe und Vorgehensweisen von Angreifern mit Softwareprogrammen automatisiert werden (vgl. Abschnitt 2). Entsprechend ist es in der digitalen Welt leicht möglich und leider auch Realität, dass ein einzelner Angreifer gleichzeitig mehrere Opfer angreift, was in der realen Welt weitgehend ausgeschlossen werden kann: Auch ein versierter Einbrecher kann nicht gleichzeitig in zwei Häuser an verschiedenen Orten eindringen. Diese Tatsachen unterstreichen die Notwendigkeit der **Umsetzung zusätzlicher Sicherheitsmaßnahmen** bei der Absicherung von IT-Systemen, um ein der realen Welt vergleichbares Maß an Sicherheit zu erreichen.

3.2. Reaktive Maßnahmen beim sicheren Betrieb von Internetportalen

In dem bereits erwähnten vom NIST (National Institute of Standards and Technology) herausgegebenen Leitfaden zur Absicherung von Web-Servern wird in Abschnitt 9.1.3 „Recommended Generic Logging Configuration" als guter Startpunkt für eine Zugriffsprotokollierung das sogenannte „Combined Log Format" genannt, welches zu jedem Zugriff neben sechs weiteren Einträgen die Adresse des zugreifenden Systems festhält (vgl. [NIST 2007]).

Insbesondere vor dem Hintergrund der durch die Ausführungen in Abschnitt 2 untermauerten gravierenden Bedrohungslage und Unsicherheit beim Betrieb von Internetportalen sind reaktive Sicherheitsmechanismen zur Absicherung von Internetportalen sowohl aus Sicht der Betreiber als auch der Nutzer unverzichtbar. Dies schließt in jedem Fall die Protokollierung von Zugriffsanforderungen und eine auf den protokollierten Daten basierende Überprüfung hinsichtlich aufgetretener Sicherheitsverletzungen - unter anderem mit automatischen Verfahren zur Angriffserkennung - ein.

<u>Ziele und Nutzen der Protokollierung und Angriffserkennung</u>

Die Protokollierung und Angriffserkennung erfolgt mit mehreren Zielsetzungen bzw. angestrebten Wirkungen:

- Z1: Protokollierung und Angriffserkennung ermöglichen die Ergreifung von Gegenmaßnahmen, beispielsweise zur Verringerung der Auswirkungen von anhaltenden Sicherheitsbeeinträchtigungen.
- Z2: Protokollierung und Auswertung der Protokolldaten nach einem Sicherheitsvorfall erlauben eine Beurteilung des eingetretenen Schadens. In Abhängigkeit vom Inhalt der Protokolldaten können insbesondere betroffene Ressourcen, betroffene Nutzer oder betroffene externe Parteien ermittelt werden.

- Z3: Durch ein Nachvollziehen erkannter Sicherheitsverletzungen anhand der Protokolldaten kann die Vorgehensweise des Angreifers rekonstruiert werden. Dies ist wesentlicher Bestandteil eines Sicherheitsprozesses. Insbesondere können dadurch neue bislang unbekannte Schwachstellen und Wege zu deren Ausnutzung erkannt werden. Ausgehend von diesen gewonnenen Informationen kann der präventive Schutz verbessert werden.
- Z4: Die Erkennung von Angriffen und die Analyse von Protokolldaten unterstützen die Ermittlung der verantwortlichen Angreifer.
- Z5: Durch den Einsatz von Protokollierung und Angriffserkennung wird eine Abschreckung von Angreifern erreicht. In dieser Hinsicht wirken diese Mechanismen ähnlich präventiv wie die Anwesenheit von Zeugen am Ort einer potentiellen Straftat.

Die hier betrachteten IT-Systeme zur Bereitstellung eines Informationsangebots (Server) sind dabei nur ein Teil der zu schützenden Umgebung. Dazu kommen insbesondere die Client-Systeme, mit denen die Server-Systeme interagieren (vgl. Abschnitt 2). Angriffe auf Server-Systeme können nur Vorstufe eines Angriffs auf Client-Systeme sein. Eine Server-seitig realisierte Angriffserkennung trägt hier insbesondere auch zum Schutz von Client-Systemen bei und erlaubt im Falle eines Angriffs die Beurteilung, wie viele und ggf. welche Client-Systeme betroffen sind. Gleiches gilt für weitere von einem Angriff betroffene Systeme.

Verfahren zur automatischen Angriffserkennung

Die meisten automatischen Verfahren zur Angriffserkennung realisieren den als Missbrauchserkennung oder Signaturanalyse bezeichneten Ansatz, bei dem Protokolldaten nach Anzeichen von konkreten Sicherheitsverletzungen durchsucht werden. Dazu verwenden sie definierte Angriffsmuster (auch als Signaturen bezeichnet). Während der Analyse werden die vorliegenden Protokolldaten auf Übereinstimmung mit den Angriffsmustern untersucht und gefundene Übereinstimmungen als Sicherheitsverletzungen angezeigt.

In Abhängigkeit vom Ablauf und dem erforderlichen Aufwand zur Erkennung können Angriffe in zwei Klassen unterteilt werden. Angriffe, die auf der Grundlage von einzelnen Zugriffsprotokolleinträgen erkannt werden können, werden als **Einzelschrittangriffe** bezeichnet. **Mehrschrittangriffe** hingegen bezeichnen Sicherheitsverletzungen, zu deren Erkennung mehrere Zugriffsprotokolleinträge in Zusammenhang gebracht und auf charakteristische Merkmale untersucht werden müssen.

Einfache **Einzelschrittangriffe** können zum großen Teil durch Zugangs- und Zugriffskontrollsysteme, z.B. eine Firewall, durch Beurteilung des einzelnen Zugriffs verhindert werden. Die komplexeren **Mehrschrittangriffe** hingegen können durch diese Systeme nicht erkannt und nicht unterdrückt werden.

Die Bedeutung von IP-Adressen bei der Angriffserkennung und -abwehr

Bei der Analyse von Zugriffsprotokolldaten besteht eine Herausforderung darin, die zu den einzelnen Schritten einer Attacke korrespondierenden Zugriffsprotokolldatensätze als zu dieser Attacke zugehörig zu erkennen. Dazu werden in Angriffsmustern **schrittübergreifende Merkmale** der einzelnen Schritte formuliert, über die ein Zusammenhang von Einzelaktionen hergestellt werden kann. Diese Merkmale sind typischerweise Ressourcen- bzw. Objekt-Identifikatoren (z.B. Dateinamen oder Prozess-IDs) oder Kennungen von Zugriffsverursachern, z.B. Nutzer-IDs oder Rechnernamen bzw. IP-Adressen. Diese **schrittübergreifenden Merkmale** müssen zwingend in den Zugriffsprotokolldaten enthalten sein, um eine darauf aufbauende Erkennung von Mehrschrittangriffen zu ermöglichen.

Bei den betrachteten Internetportalen ist es unverzichtbar, IP-Adressen in Zugriffsprotokolldaten festzuhalten, um Angriffsmuster zur Erkennung von Mehrschrittangriffen überhaupt formulieren und erkennen zu können. Das Stattfinden von Mehrschrittangriffen manifestiert sich in der Erstellung von Zugriffsprotokolleinträgen zu den einzelnen Zugriffen/Schritten, deren schrittübergreifende Merkmale einer angriffsspezifischen **Inter-Schritt-Bedingung** genügen, also beispielsweise einen gleichen Wert enthalten. Zur Absicherung von Internetportalen verwenden viele Angriffsmuster die IP-Adressen zugreifender Systeme als schrittübergreifendes Merkmal und entsprechende Inter-Schritt-Bedingungen fordern, dass diese IP-Adressen dem gleichen Teilnetz angehören oder gleich sind oder anderweitig in (angriffs-)spezifischer Relation stehen.

Ein Verzicht auf die Protokollierung von IP-Adressen würde hier die Formulierung entsprechender Angriffsmuster als Auslöser von Alarmen unmöglich machen. Bei der Formulierung von Angriffsmustern müsste auf die Spezifikation von IP-Adress-bezogenen Inter-Schritt-Bedingungen verzichtet werden, was in viel zu allgemeinen Mustern resultieren würde, deren Anwendung eine Flut von Fehlalarmen durch die Angriffserkennungssysteme zur Folge hätte.

Ein (leider sehr reales) Beispiel: *Im Umfeld der Erpressung von Betreibern von Internetportalen ist heute folgende Vorgehensweise an der Tagesordnung: Werden erpresste Geldbeträge von den Portalbetreibern nicht bezahlt, so wird die Erreichbarkeit der Internetportale eingeschränkt, indem die Portale beispielsweise unter Verwendung von Botnetzen mit Zugriffsanfragen überflutet werden. Oftmals werden dabei nicht nur die Portale der erpressten Unternehmen, sondern auch deren Unterstützer, also Internet-Service-Provider und Ermittlungsbehörden, Ziel dieser Angriffe und dadurch von den Tätern für ihr Eingreifen abgestraft. Gerade weil die Abwehrmöglichkeiten hier sehr begrenzt sind und um den Tätern nicht völlig das Feld zu überlassen, ist es unverzichtbar, eine Protokollierung der Portalzugriffe inklusive IP-Adressen vorzunehmen. Ausgehend von dieser Protokollierung können dann Analysen vorgenommen werden, beispielsweise bezogen auf die Frage, ob es Systeme gibt, die kurz vor und kurz nach einer Denial-of-Service-Attacke (siehe 2.1.1.) die Erreichbarkeit eines Portals durch einen Zugriff getestet haben und ob in verschiedenen*

Erpressungsfällen bestimmte IP-Adressen oder IP-Adressbereiche immer wieder auftauchen...

Folglich ist die Protokollierung von IP-Adressen bei der Absicherung von Internetportalen ein zentrales Mittel. Auch für die anderen oben genannten Ziele der Protokollierung und Angriffserkennung, die über die bloße Erkennung von Sicherheitsvorfällen hinausgehen, ist das Vorliegen der IP-Adresse in den Protokolldaten zwingende Voraussetzung.

Oftmals sind Angriffe auf Internetportale nur ein Mittel zu dem Zweck, die Besucher der Portale anzugreifen. Sofern Besucher dem Portal Informationen übermitteln, und mit zunehmender Verbreitung von e-Government-Diensten ist von der Übermittlung sensitiver Daten an entsprechende Portale des Bundes auszugehen, kann der Angreifer auf Seiten des Portals diese Informationen abgreifen. Gleichzeitig können Angreifer ein Portal derart manipulieren, dass Besucher der Webseite mittels der in Abschnitt 2 bereits beschriebenen Drive-By Infections attackiert werden. Die Beurteilung der Auswirkungen eines Angriffs bzw. des verursachten Schadens (vgl. Z2 oben) schließt bei Internetportalen also die Auswirkungen und den Schaden auf Seiten der Portal-Besucher mit ein. Nach Entdeckung einer Manipulation des Internetportals kann auf der Grundlage von Zugriffsprotokollen mit IP-Adressen durch ein Zählen unterschiedlicher IP-Adressen beurteilt werden, wie viele Besucher das manipulierte Portal hatte, also wie viele Systeme dem Informationsabfluss bzw. der Drive-By Infection potentiell zum Opfer gefallen sind. Außerdem kann ermittelt werden, von welchen konkreten IP-Adressen auf das manipulierte Portal zugegriffen wurde, so dass über die Internet Service Provider die Möglichkeit besteht, die Opfer zu informieren. Zwar ist nicht in jedem Fall eine direkte Information der Nutzer einer IP-Adresse möglich und sinnvoll, aber der für die jeweiligen IP-Adressen verantwortliche Internet-Service-Provider kann informiert werden und entsprechende Informationen an seine Nutzer bzw. Kunden weiterleiten, um diese zu warnen.

Es liegt im Interesse der Internet-Service-Provider, ihre Kunden bzw. Nutzer über deren Betroffenheit von entsprechenden Angriffen zu informieren oder selbst zusätzliche Sicherheitsmaßnahmen zu ergreifen – beispielsweise auch die Blockierung einzelner Dienste von Kundenrechnern, von denen aufgrund von Schad-Softwareinfektionen Angriffe ausgehen. Um diesem Interesse gerecht zu werden, ist es gängige Praxis, dass Internet-Service-Provider auch selbst aktiv auf externe Informationsquellen zugreifen, um ausgehend von im Zusammenhang mit protokollierten Sicherheitsvorfällen vorliegenden IP-Adressen ihre Kunden entsprechend informieren zu können. Zu diesem Zweck unterhalten Internet-Service-Provider sogenannte „Abuse Teams".

Wie bereits in Abschnitt 2 erwähnt, hat das Abuse Team der Deutschen Telekom im ersten Halbjahr 2012 insgesamt 137.237 Kunden darüber informiert, dass ihre Computer vermutlich mit Schad-Software infiziert sind. Im gleichen Zeitraum wurden bei 48.582 Kunden der Deutschen Telekom aus Sicherheitsgründen Netzwerkdienste blockiert [DTAG 2012].

Schon heute ist es dringend wünschenswert, die Besucher eines kompromittierten Portals über ihre Betroffenheit und über Auswirkungen der Manipulation am besuchten Portal informieren zu können. Eine derartige Information von Betroffenen war in der Vergangenheit vollkommen unüblich, ist aber – wie beschrieben - bei guten Internet Service Providern bereits heute gängige Praxis, wenn auch in eingeschränktem Umfang. Für die Weiterentwicklung der dringend notwendigen Schutzmechanismen bis hin zu den ebenfalls bereits angesprochenen Blockierungen von Netzdiensten zum Schutz der übrigen Systeme – hier ist eine gewisse Vergleichbarkeit mit Quarantäne-Stationen gegeben – ist die vorherige Protokollierung der IP-Adressen unverzichtbar.

An dieser Stelle sei angemerkt, dass seriöse Internet-Service-Provider wie die Deutsche Telekom auch Schutz vor IP-Spoofing, also dem gezielten Fälschen von IP-Absender-Adressen, realisieren. Insbesondere im Bereich der privaten xDSL-Kunden wird typischerweise ein Spoofing-Schutz auf der Basis einer Technik namens uRPF (Unicast Reverse Path Forwarding [RFC 3704]) realisiert. Wenn vom Computer des Kunden eines entsprechenden Internet-Service-Providers Netzwerkverkehr mit gefälschter Absender-IP-Adresse versendet wird, so wird dieser am Zugangs-Router des Internet-Service-Providers erkannt und konsequent verworfen.

3.3. Verwendung von Pseudonymen

In der wissenschaftlichen Literatur (vgl. z.B. [FLEGEL 2006]) wird vorgeschlagen, bei der Protokollierung von Zugriffsanforderungen solche Merkmale, die unter Umständen vertraulich behandelt werden sollen oder müssen, nicht im Klartext zu speichern sondern durch Stellvertreterwerte, oft als **Pseudonyme** bezeichnet, zu ersetzen, um einerseits die Vertraulichkeit dieser Merkmale zu schützen und gleichzeitig die Verfügbarkeit von Protokolldaten für eine Angriffserkennung zu gewährleisten. Eine Zuordnungsregel ordnet dabei jedem Pseudonym eindeutig das dadurch ersetzte Merkmal zu. Ein solches Merkmal kann durch verschiedene Pseudonyme ersetzt werden.

Es ist Gegenstand der aktuellen Forschung, Pseudonyme derart zu generieren, dass die im Verlauf einer Angriffserkennung erforderlichen Analysen auch auf diesen Pseudonymen korrekt durchgeführt werden können und im Falle erkannter Sicherheitsverletzungen auch zielgerichtete Gegenmaßnahmen möglich bleiben. Zwei Eigenschaften von Pseudonymen sind hierbei wesentlich – ihre Aufdeckbarkeit und ihre Verkettbarkeit.

Die **Aufdeckbarkeit** von Pseudonymen stellt eine kontrollierte Möglichkeit dar, Pseudonyme (wieder) durch ihre Klartextmerkmale zu ersetzen. Diese Möglichkeit kann über die Kenntnis der Zuordnungsregel kontrolliert werden. In der Literatur finden sich sowohl Vorschläge für Ansätze zur organisatorischen als auch technischen Kontrolle der Kenntnis der Zuordnungsregel. Bei **organisatorischer Kontrolle** wird die Verantwortung über den Umgang mit der Zuordnungsregel einer Person oder Personengruppe übertragen. Bekannte Ansätze zur **technischen Kontrolle** lassen bereits bei der Pseudonymkonstruktion die Zuordnungsregel in geschützter Form in die Pseudonyme

einfließen. Unter definierten Bedingungen wird dieser Schutz unwirksam. Entsprechend sind die Pseudonyme bei Vorliegen dieser Bedingungen aufdeckbar, anderenfalls sind sie nicht aufdeckbar.

Die **Verkettbarkeit** von Pseudonymen liefert die Möglichkeit zu überprüfen, ob zwei Pseudonyme oder ein Pseudonym und ein Wert zueinander in Relation stehen, also beispielsweise gleich sind, oder ein Pseudonym kleiner ist als das andere, oder ob beide einer bestimmten Gruppe zugehören. Entsprechend ist die Verkettbarkeit für all jene Relationen zu betrachten, die während der Analyse der pseudonymisierten Daten überprüft werden.

Die zentrale Herausforderung besteht darin, Pseudonyme derart verkettbar zu gestalten, dass einerseits eine Analyse der Protokolldaten hinsichtlich ausgeführter Angriffe anhand von Angriffsmustern weiterhin möglich ist, und andererseits für den Fall, dass eine Sicherheitsverletzung erkannt wurde, die Aufdeckung von Pseudonymen unterstützt wird.

Anforderungen an Pseudonyme für IP-Adressen

Damit eine Zugriffsprotokollierung und Angriffserkennung die oben dargestellten Ziele und Wirkungen erreichen kann, bestehen hinsichtlich Verkettbarkeit und Aufdeckbarkeit folgende Anforderungen an Pseudonyme für IP-Adressen.

- A1. Da Inter-Schritt-Bedingungen in Angriffsmustern zur Erkennung von Mehrschrittangriffen IP-Adressen auf verschiedene Relationen (z.B. Gleichheit oder Zugehörigkeit zum gleichen Teilnetz) überprüfen, müssen Pseudonyme für IP-Adressen bezüglich all dieser Relationen verkettbar sein, damit diese Bedingungen auch auf den Pseudonymen korrekt überprüft werden können.
- A2. Zur Gewährleistung einer effektiven Abschreckung sowie zur Ergreifung von Gegenmaßnahmen müssen die Pseudonyme für IP-Adressen, die in den Angriff involviert sind und dem Angreifer oder zumindest einem am Angriff beteiligten System zuzurechnen sind, im Fall eines erkannten Angriffs aufdeckbar sein.
- A3. Um eine Beurteilung der durch einen Angriff eingetretenen Schäden, eine Ermittlung und Information der betroffenen Portal-Besucher (bzw. zunächst deren Internet-Service-Provider) sowie die Ergreifung Schaden-eindämmender Gegenmaßnahmen (z.B. die Blockierung infizierter System) zu ermöglichen, müssen die Pseudonyme der IP-Adressen der Besucher des manipulierten Portals aufdeckbar sein. Hierbei handelt es sich um IP-Adressen von Portal-Besuchern, deren Portalzugriffe zunächst nichts mit dem eigentlichen Angriff auf das Portal zu tun haben, die jedoch Opfer der vom manipulierten Portal ausgehenden Folgeangriffe sind.

Stand der Wissenschaft

In der wissenschaftlichen Literatur gibt es eine Reihe von Vorschlägen, wie eine Zuordnungsregel implementiert werden kann und wie Pseudonyme derart konstruiert werden können, dass Sie hinsichtlich spezifischer Relationen verkettbar sind. Die bereits vom Gutachter Köpsell angeführte Dissertation [Flegel2006] von Prof. Dr. Ulrich Flegel liefert einige Beiträge zum Thema Angriffserkennung auf pseudonymisierten Protokolldaten, die in spezifischen Anwendungskontexten anwendbar sind.

Dazu zählt die technisch kontrollierte Aufdeckung von Pseudonymen, die an einfache Aufdeckungsbedingungen gebunden ist. Die Idee hierbei ist, die in einfachen Angriffsmustern formulierten Bedingungen als Aufdeckungsbedingung zu verwenden: Ist das Angriffsmuster aufgetreten und somit die Aufdeckungsbedingung erfüllt, so sind die **involvierten Pseudonyme** aufdeckbar. In anderen Fällen sind die Pseudonyme nicht aufdeckbar. Dieser Ansatz funktioniert jedoch zunächst **nur für sehr einfache Angriffsmuster**, die lediglich eine bestimmte Häufigkeit eines Zugriffs beschreiben („Zugriff X ist 5 mal aufgetreten"). Um das mehrfache Auftreten eines Zugriffs zu erkennen, genügt es, wenn die protokollierten Zugriffe und darin enthaltene Pseudonyme bezüglich der Gleichheitsrelation verkettbar sind, was durch den vorgestellten Ansatz gewährleistet ist. Eine Verkettung bezüglich weiterer Relationen, wie sie obige Anforderung A1 fordert, wird jedoch nicht betrachtet. Eine Aufdeckbarkeit von Pseudonymen in protokollierten Zugriffen, die mit dem Angriffsmuster nicht in Zusammenhang stehen, wie sie jedoch von obiger Anforderung A3 gefordert ist, wird von dem Ansatz nicht betrachtet und nicht unterstützt.

In der genannten Dissertation wurden außerdem umfangreiche Versuche unternommen, technisch kontrollierte Aufdeckung von Pseudonymen an komplexe Aufdeckungsbedingungen, die komplexen Angriffsmustern entsprechen, zu binden, und gleichzeitig die Verkettbarkeit von Pseudonymen auf das zur Angriffserkennung erforderliche Minimum zu reduzieren. Die gelingt jedoch nur teilweise. So wird zwar zunächst ausgehend von realen Angriffsmustern diskutiert, letztlich wird aber ein vereinfachtes Modell von Angriffsmustern zugrunde gelegt, in dem Angriffsmuster und damit die Aufdeckungsbedingungen **nur annähernd** erfasst werden können. Verkettbarkeit wird ausschließlich für die Gleichheitsrelation betrachtet. Andere Relationen werden auf Pseudonymen nicht unterstützt, was zu einer dramatischen Einschränkung der effektiv formulierbaren Angriffsmuster bzw. Aufdeckungsbedingungen führt und obige **Anforderung A1 unerfüllt** lässt.

Es sind keine Arbeiten bekannt, die die verbliebenen Lücken schließen und obigen Anforderungen an Pseudonyme für IP-Adressen genügen. Hier besteht weiterer Forschungsbedarf.

Die bisherigen wissenschaftlichen Arbeiten verfolgen das erstrebenswerte Ziel, auf der Grundlage von Pseudonymen einen fairen anwendungsspezifischen Kompromiss zwischen den in Konflikt stehenden Interessen Vertraulichkeit und Verfügbarkeit/Zurechenbarkeit von Merkmalen von Protokolldaten zu erreichen. Nach

aktuellem Stand der Forschung sind die vorgeschlagenen Ansätze aber nur für wenige Spezialfälle und nicht für praktisch relevante Anwendung einsetzbar.

Darüber hinaus kollidieren weitere Eigenschaften der existierenden Ansätze mit den Anforderungen des praktischen Einsatzes. Die folgenden Fakten schließen derzeit eine Protokollierung von IP-Adressen ausschließlich unter Pseudonymen aus:

Die Ersetzung von Merkmalen durch Pseudonyme führt zu einer **Änderung des Datenformats** der Protokolldaten. Ursache hierfür ist unter anderem, dass in Pseudonymen Metainformation eingebettet wird – im Falle technisch kontrollierter Aufdeckbarkeit sind dies beispielsweise Teile der Zuordnungsregel. Entsprechend gelingt es nicht, das Pseudonym für eine 4 Byte große IP-Adresse wiederum als 4 Byte große Pseudo-IP-Adresse zu repräsentieren. Dies hat die unangenehme Konsequenz, dass existierende Datenanalysewerkzeuge und Einbruchserkennungssysteme auf pseudonymisierten Daten nicht mehr eingesetzt werden können. Neben dem erhöhten Speicheraufwand für Pseudonyme muss auch die erhöhte Rechenzeit zur Erstellung der Pseudonyme sowie zur Analyse pseudonymisierter Daten berücksichtigt werden, die durchaus eine signifikante Aufrüstung entsprechender Systeme erforderlich machen würde. Des Weiteren sind selbst die erforschten Ansätze zur Pseudonymisierung von Protokolldaten noch nicht in Produkte eingeflossen: **Dem Gutachter sind keine marktverfügbaren Produkte bekannt**, welche die verfügbaren Ansätze zu Pseudonymisierung und Analyse pseudonymer Daten unterstützen.

Da in Anbetracht der Sicherheitslage nicht auf das zentrale Mittel IP-Adresse verzichtet werden kann, und keine adäquaten Pseudonymisierungsansätze für den praktischen Einsatz verfügbar sind, ist die Speicherung von IP-Adressen in Klartextformat nach dem Stand der Technik unverzichtbar.

4. Würdigung der Argumente des Herrn Sachverständigen Dr.-Ing. Köpsell

Im Folgenden gehe ich auf ausgewählte Ausführungen des Gutachters Dr.-Ing. Köpsell ein, die aus meiner Sicht nicht unkommentiert bzw. unwidersprochen bleiben können.

Zum Gutachten von Dr.-Ing. Köpsell vom 29. Juli 2011, S. 7:

Im Zusammenhang mit Angriffserkennungsverfahren stellt Gutachter Köpsell dar, dass nicht immer anhand eines einzelnen IP-Pakets, sondern vielmehr erst anhand einer Menge zusammengehöriger IP-Pakte entschieden werden kann, ob es sich um einen Angriffsversuch handelt oder nicht, und hier die IP-Adressen zur Beurteilung der Zusammengehörigkeit von IP-Paketen benötigt werden. Er führt weiter aus, dass anstatt der IP-Adressen andere Ersetzungskennzeichen verwendet werden können. **Falsch** ist der Eindruck, den der Gutachter erweckt, wenn er anmerkt, dass *„ ... das Ersetzungskennzeichen selbst wieder aus der Menge gültiger IP-Adressen stammen kann."*.

Dies trifft auf die in der wissenschaftlichen Literatur einschlägig vorgeschlagenen Ersetzungsverfahren einschließlich der - vom Gutachter angeführten - in der Dissertationsschrift von Prof. Dr. Flegel beschriebenen Verfahren **nicht** zu, wie bereits in Abschnitt 3.3 ausgeführt wurde.

Der Gutachter führt an gleicher Stelle weiter aus: *„Auf diese Weise lassen sich vorhandene Systeme zur Angriffserkennung und -abwehr prinzipiell weiter verwenden, da sich das Datenformat eines IP-Paketes nicht ändert."*

Der vom Gutachter mit diesen Ausführungen vermittelte Eindruck, dass auf Klartext-Protokolldaten operierende Angriffserkennungssysteme gleichermaßen effektiv und effizient auf Daten operieren können, in denen IP-Adressen durch Ersetzungskennzeichen (Pseudonyme) ersetzt wurden, ist **nicht zutreffend** (vgl. obigen Abschnitt 3.3). Insbesondere hat Prof. Dr. Flegel in seinen Arbeiten zur Dissertation **nicht** auf existierende Angriffserkennungssysteme zurückgegriffen, sondern eigene neue Systemprototypen entwickelt.

Die Ausführungen des Gutachters Köpsell hinsichtlich der praktischen Auswirkungen einer Verwendung von Pseudonymen bzw. Ersetzungskennzeichen wirken also als „beschönigte" Darstellung zum Stand der Wissenschaft bzw. Technik.

Zum Gutachten von Dr.-Ing. Köpsell vom 29. Juli 2011, S. 9 sowie seinen Erläuterungen zum Gutachten vom 7. Mai 2012, S. 3:

Der Gutachter führt aus:

„Ein Beispiel aus der ‚offline Welt' mag dies verdeutlichen: Überlicherweise werden zum Zutrittsschutz bei Wohnungen, Häusern oder Autos verschlossene Türen verwendet. Wohingegen der Vorschlag, einfach Türen offen stehen zu lassen und statt dessen ausschließlich Überwachungskameras zu installieren, wohl auf wenig Akzeptanz stoßen dürfte."

Der Gutachter führt an anderer Stelle aus:

„Ich bezeichne insbesondere ein IT-System nicht als sicher, welches lediglich versucht nach dem Eintreten eines Schadens den Schadensverursacher zu ermitteln, um im Zuge des Schadenersatzes den tatsächlich aufgetretenen Gesamtschaden zu minimieren."

Zwar kann ich mich den Ausführungen des Gutachters Köpsell anschließen, ich frage mich jedoch, woher der offensichtlich unsinnige Vorschlag, den der Gutachter hier diskutiert, stammt, warum er vom Gutachter wiederholt thematisiert wird und was er damit bezweckt. Wie in meiner Stellungnahme umfassend erläutert, ist es für den professionellen Betrieb von Internet-Portalen zwingend erforderlich, **sowohl präventive** Schutzmechanismen („Einbruchschutz") **als auch reaktive Maßnahmen** einzusetzen, um insgesamt ein akzeptables Schutzniveau erreichen zu können.

Zu den Erläuterungen zum Gutachten von Dr.-Ing. Köpsell vom 7. Mai 2012, S. 11:

Der Behauptung des Gutachters, dass *„der Betrieb eines Intrusion Detection Systems bzw. ähnlicher Systeme, die für eine sinnvolle Funktionsweise einen Rückgriff auf gespeicherte Daten benötigen ... nicht zwingend notwendig für den sicheren Betrieb eines IT-Systems [ist]."* **muss widersprochen werden** (vgl. meine Ausführungen in Abschnitt 3). Wenn der Gutachter wirklich das meint, was dieser Text aussagt, dann hat er die Funktionsweise und Wirkung von Intrusion Detection Systemen bzw. Angriffserkennungssystemen nicht verstanden.

5. Resümee

Aufgrund der massiven technischen Unzulänglichkeiten vernetzter IT-Systeme muss davon ausgegangen werden, dass öffentliche Internetportale permanent angegriffen werden und trotz sorgfältigem Betrieb nach dem jeweils aktuellen Stand der Technik prinzipiell jederzeit durch Angreifer kompromittierbar sind. Dies gilt in besonderem Maße – aber keineswegs ausschließlich - für interaktive Angebote im Rahmen des sog. Web 2.0. Um ein akzeptables Maß an Sicherheit zu erreichen, ist es zwingend notwendig, in Ergänzung präventiver Sicherheitsmaßnahmen auch reaktive Sicherheitsmaßnahmen einzusetzen.

Internetportale sind oft nur Zwischenziel von Angriffen, die letztlich auf die Besucher der Internetportale abzielen – seien dies nun Mitarbeiter der für den Betrieb verantwortlichen Einrichtung oder externe Besucher. Existierende Richtlinien zur Absicherung von Internetportalen bzw. Webservern empfehlen die Protokollierung der Zugriffe auf den Web-Server einschließlich der zugreifenden IP-Adresse sowie eine Analyse der Protokolldaten hinsichtlich aufgetretener Angriffe. Zitiert sei hier aus [NIST 2007], Abschnitt 8.2.2. „Intrusion Detection and Prevention Systems", S. 8-10, 8-11:

> „To successfully protect a Web server using an IDPS, ensure that the IDPS is configured to monitor network traffic to and from the Web server, ... log events, including the following details
>
> - Time/date
> - ...
> - Source and destination IP addresses"

Die Analyse von Zugriffsprotokolldaten verfolgt mehrere Zielsetzungen. Wichtigstes Ziel ist es, die durch einen erfolgreichen Angriff verursachten Schäden zu beurteilen und betroffene Opfer zu informieren. Außerdem soll die Vorgehensweise der Angreifer analysiert werden mit dem Ziel, den präventiven Schutz immer weiter zu verbessern. Eine derartige ständige Weiterentwicklung des präventiven Schutzes ist zwingend erforderlich, weil auch die Methoden der Angreifer immer weiter verbessert werden. Schließlich soll die Ergreifung von Gegenmaßnahmen zur Verringerung der Auswirkungen von Angriffen ermöglicht werden (Schadensbegrenzung, „Resilienz"). Zur Erreichung dieser Zielsetzungen sind im Zusammenhang mit dem Schutz von Internetportalen die IP-Adressen der zugreifenden Systeme ein zentrales Mittel und eine Protokollierung dieser IP-Adressen ist unverzichtbar.

Die in der wissenschaftlichen Literatur vorgeschlagenen Ansätze zur Ersetzung der IP-Adressen in den Protokolldaten durch Pseudonyme sind (heute und auf absehbare Zeit) nicht für den praktischen Einsatz zur effektiven Angriffserkennung und –abwehr geeignet. Angriffserkennungssysteme, die derartige Ansätze umsetzen und auf professionellen Betrieb ausgerichtet sind, sind am Markt nach Kenntnisstand des Gutachters nicht verfügbar.

Referenzen

[BISKUP 2009]
J. Biskup, **"Security in Computing Systems - Challenges, Approaches and Solutions"**
Springer Verlag, 2009, ISBN: 978-3-540-78441-8

[BSI 2012]
BSI, **"Kritische Sicherheitslücke in Java-Version 7 wird ausgenutzt"**
Bundesamt für Sicherheit in der Informationstechnik, Pressemitteilung, 28.8.2012
https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2012/Sicherheitsluecke-in-Java-Version_28082012.html

[DTAG 2012]
Deutsche Telekom, **"Sicherheit im Internet – Bericht zur Informations- und Internetsicherheit"**
Deutsche Telekom, Group IT Security and P&I Abuse, August 2012
http://www.telekom.com/static/-/137064/6/pdf-sicherheit-im-internet-aug-12-si

[ENISA 2012]
ENISA, **"<<High-Roller>> Online-Bankeinbrüche entlarven Sicherheitslücken"**
EU-Intersicherheitsagentur ENISA: Flash Note – Pressemitteilung, 5. Juli 2012,
http://www.enisa.europa.eu/media/press-releases/eu-internetsicherheitsagentur-enisa-high-roller-online-bankeinbruche-entlarven-sicherheitslucken

[FLEGEL 2006]
U. Flegel, **"Pseudonymizing Audit Data for Privacy Respecting Misuse Detection"**
Dissertation, Fakultät für Informatik, Universität Dortmund, January 2006.

[HEISE 2011]
Heise Security, **"Tool bringt Apache-Webserver zum Stillstand"**
Heise News Meldung, 24.8.2011
http://www.heise.de/security/meldung/Tool-bringt-Apache-Webserver-zum-Stillstand-1329986.html

[HP 2011]
Hewlett-Packard, **"2011 Top Cyber Security Risks Report"**,
Hewlett-Packard Development Company, Technical White Paper, September 2011
http://www.hpenterprisesecurity.com/collateral/report/2011FullYearCyberSecurityRisksReport.pdf

[KOSS 2000]
K.-P. Kossakowski und J. Allen, **"Securing Public Web Servers"**, Carnegie Mellon Software Engineering Institute, CMU/SEI-SIM-011, April 2000
http://www.sei.cmu.edu/library/abstracts/reports/00sim011.cfm

[NIST 2007]
NIST, **"Guidelines on Securing Public Web Servers – Recommendations of the National Institute of Standards and Technology"**
NIST – National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-44 Version 2, September 2007
http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf

[PLONE 2012]
Plone, **"Security vulnerability announcement: 20120830 – Multiple vectors"**
Plone Security Advisory, 1. November 2012
http://plone.org/products/plone/security/advisories/20120830
Diese Seite ist online nicht mehr verfügbar; Anfragen werden umgeleitet auf
http://plone.org/products/plone/security/advisories/20121106-announcement

[RFC 3704]
F. Baker, P. Savola, **„Ingress Filtering for Multihomed Networks "**
RFC 3704, The Internet Society, 2004.

Anlage BB 6

Institut für Informatik 4
Arbeitsgruppe Kommunikationssysteme
Universität Bonn

Prof. Dr. Peter Martini

Seit dem Wintersemester 1996/97 leitet Prof. Dr. Peter Martini das Institut für Informatik 4 der Universität Bonn und die dort beheimatete Arbeitsgruppe Kommunikationssysteme. Dieser Arbeitsgruppe gehören 16 wissenschaftliche Mitarbeiter, drei Techniker, eine Sekretärin und ca. 30 studentische Hilfskräfte an (Stand: Februar 2009).

1. Das Institut für Informatik 4

Das Institut für Informatik der Universität Bonn ist in insgesamt sechs Abteilungen strukturiert. Der Abteilung 4 des Instituts, die sich mit Kommunikation und Verteilten Systemen befasst, gehören die Arbeitsgruppe „Kommunikationssysteme" unter Leitung von Prof. Dr. Peter Martini und die Arbeitsgruppe „Sensornetze und Pervasive Computing" unter Leitung des im Jahr 2007 nach Bonn berufenen Prof. Dr. Pedro José Marrón an. Gemeinsam decken die eng kooperierenden Gruppen in Forschung und Lehre ein breites Spektrum der praktischen und anwendungsorientierten Informatik ab.
Da in beiden Gruppen der Praxisbezug im Vordergrund steht, dieser aber nur mit starken Partnern sichergestellt werden kann, bestehen enge Verbindungen sowohl zur gewerblichen Wirtschaft als auch zu den im Bereich des Technologietransfers tätigen Großforschungseinrichtungen. Besondere Bedeutung haben hierbei das Fraunhofer Institut „Intelligente Analyse- und Informationssysteme" (IAIS) in St. Augustin und das „Forschungsinstitut für Kommunikation, Informationsverarbeitung und Ergonomie" (FKIE) der Forschungsgesellschaft für Angewandte Naturwissenschaften (FGAN) in Wachtberg: Mit diesen beiden renommierten Instituten bestehen langfristig angelegte Kooperationsverträge, welche die Basis für die enge personelle Verknüpfung und die umfassenden gemeinsamen Lehr- und Forschungsaktivitäten darstellen. Auch mit dem Fraunhofer Institut Algorithmen und Wissenschaftliches Rechnen (SCAI), ebenfalls in St. Augustin, besteht seit vielen Jahren eine enge Kooperation.
Essentiell ist auch die enge Zusammenarbeit mit dem Bonn-Aachen International Center for Information Technology (B-IT). In mehreren international ausgerichteten Studiengängen sind dort die Studierenden stark in die Labore der beteiligten Einrichtungen (Universität Bonn, RWTH Aachen, mehrere Fraunhofer-Institute) eingebunden, was eine sowohl forschungsnahe als auch praxisorientierte Ausbildung sicherstellt. Darüber hinaus bietet das B-IT mit dem „International Program of Excellence in Computer Science" (IPEC) besonders hoch begabten Studierenden die Möglichkeit, durch Blockveranstaltungen in der vorlesungsfreien Zeit ihr Studium signifikant zu verkürzen. Das Institut für Informatik 4 ist mit einem breiten Angebot von Praktika, Vorlesungen und Projektgruppen sehr stark an den Aktivitäten des B-IT beteiligt.

2. Forschung

Die Forschung der Arbeitsgruppe Kommunikationssysteme gliedert sich in insgesamt vier Bereiche, die jeweils von einem wissenschaftlichen Mitarbeiter geleitet werden.

- Sicherheit und Effizienz im Internet
- Taktische Multi-Hop-Netze
- Dynamische Ende-zu-Ende-Netzdienste
- Performance Engineering

Im Tagesgeschäft folgt aus der Praxisorientierung eine starke Ausrichtung auf Kooperationsmöglichkeiten und Projektchancen, wobei recht häufig Forschungsbedarfe

primär dadurch erkannt werden, dass sich prototypische Implementierungen im Rahmen eigener Projekte oder im Rahmen von Projekten der Kooperationspartner nicht wirklich als „proof of concept" erweisen, sondern als „proof of need for further research".
Der Schnelllebigkeit dieses Tagesgeschäfts steht die Langfristigkeit der Ausrichtung der oben genannten Forschungsbereiche gegenüber: Sie bilden eine stabilisierende Struktur, in der Kompetenzen der Arbeitsgruppe über die Tätigkeit einzelner Personen und über die Bedarfe einzelner Projekte hinaus herangebildet, gepflegt und bewahrt werden. Auf diese Weise wird auch sichergestellt, dass die in der Arbeitsgruppe tätigen Studierenden stabile Arbeitsumgebungen vorfinden und ohne Umwege in kurzen Studienzeiten ihre Abschlüsse erzielen können.

2.1. Sicherheit und Effizienz im Internet

Der von dem Malware-Spezialisten Dipl.-Inform. Felix Leder geleitete Bereich umfasst Forschungsaktivitäten, die darauf abzielen, den Betrieb von Komponenten im Internet bzw. ans Internet angeschlossener Endgeräte sicherer und effizienter zu gestalten, indem Bedrohungen und Unzulänglichkeiten systematisch erkannt, klassifiziert und – nach Möglichkeit – behoben werden. Aufgrund der praxisorientierten Ausrichtung dieser Forschungsaktivitäten treten neben zahlreiche anspruchsvolle technische und mathematisch-theoretische Fragen auch Fragen nach rechtlichen und wirtschaftlichen Aspekten, die nur in strategischer Partnerschaft mit Behörden und gewerblicher Wirtschaft erfolgreich bearbeitet werden können.

2.1.1. Intrusion Detection und Honeypots

IT-Systeme im Internet sind ständigen Angriffen ausgesetzt. Zur Unterscheidung legitimer und bösartiger Zugriffe werden Angriffserkennungssysteme (Intrusion Detection Systems, IDS) eingesetzt, die Attacken anhand hinterlegter Muster oder anormaler Netzwerkdaten identifizieren und dann Alarm geben oder Schutzmaßnahmen ergreifen sollen. Zur Gewinnung dieser Muster und zur fundierten Beurteilung des jeweiligen Bedrohungspotentials erweisen sich „Honeypots" als außerordentlich nützlich. Honeypots sind i.W. „Opfer-Systeme", die in kontrollierter Weise Angriffe aufzeichnen und somit tiefe Einblicke in die Vorgehensweise der Hacker und in die Funktionsweise der verwendeten Schad-Software, der sog. Malware, zulassen.
Die Arbeitsgruppe Kommunikationssysteme ist zwar schon seit über 10 Jahren in dem hier angesprochenen Bereich aktiv, doch wurden diese Aktivitäten seit 2007 aufgrund der wachsenden Bedeutung massiv intensiviert und mit Unterstützung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf eine breitere Basis gestellt.
Als zentrale Komponente umfassender praxisorientierter Forschungsarbeiten betreibt die Arbeitsgruppe ein System verschiedener Honeypots mit Sensoren in den Bereichen verschiedener Internetprovider. Wichtige Informationen werden auch über Sensoren an diversen Messpunkten der Universität Bonn sowie durch die intensive Einbindung in die nationale und internationale „Honeynet-Community" gewonnen. Einige Honeypot-Komponenten, die von Mitgliedern der Arbeitsgruppe entwickelt wurden, befinden sich weltweit im Einsatz.
Ein besonderes Highlight stellte im Jahr 2008 die Verleihung des AFCEA-Studienpreises an den damaligen Diplomanden und jetzigen wissenschaftlichen Mitarbeiter Tillmann Werner dar. Seine Arbeit zum Thema „Automatisches Generieren komplexer Intrusion-Detection-Signaturen" zeigt neue Wege auf, wie aus aufgezeichneten Angriffsdaten automatisch Detektionsmuster berechnet werden können, die dann unmittelbar in Systemen zur Angriffserkennung einsetzbar sind und so auch Schutz vor bisher unbekannten Attacken bieten können.

2.1.2. Analyse von Malware

Eng verknüpft mit dem Bereich Honeypots sind die Aktivitäten zur „tiefen" Analyse der erfassten Malware. Dabei kommen Methoden zum Einsatz, die sich nicht auf das Beobachten des Verhaltens im Sinne eines Black Box – Ansatzes beschränken, sondern mittels Reverse Engineerings die Funktionalität von Malware extrahieren, mit Details des Laufzeit-Verhaltens kombinieren und so ein tiefes Verständnis des analysierten Schadprogramms ermöglichen. Hiermit wird auch eine Basis geschaffen für die Klassifikation von „polymorpher" bzw. „metamorpher" Malware, also von Schad-Code, der sich automatisch und zum Teil sehr schnell verändert, um der Entdeckung durch Intrusion Detection Systeme bzw. Viren-Scanner zu entgehen.

Das aus Sicht der Arbeitsgruppe wichtigste Einsatz-Szenario für die hier angesprochenen Methoden liegt im Bereich der Bekämpfung der inzwischen allgegenwärtigen „Botnetze" mit zum Teil Millionen von Zombie-Rechnern. Derartige Systeme sind inzwischen ein Tummelplatz der organisierten Kriminalität und eine massive Bedrohung für die Allgemeinheit.

Einen besonders spektakulären Erfolg, der über Medienportale wie „Heise" oder „The Register" national wie international gemeldet wurde, konnte mit der Analyse des „Sturmwurm-Botnetzes" (kurz: Storm) erzielt werden: In einer Live-Demonstration auf dem Chaos Communication Congress 2008 präsentierten Mitglieder der Arbeitsgruppe das Eindringen in die Kontrollstruktur des Storm Botnetzes, das wegen der eingesetzten Peer-to-Peer-Technik lange Zeit als unaufhaltsam galt. Die Analyse der von Storm eingesetzten Malware hatte es der Arbeitsgruppe in Kooperation mit Forschern an der RWTH Aachen aber ermöglicht, nicht nur die Funktionsweise komplett zu verstehen, sondern auch alle Software-Komponenten zu erstellen, die zur vollständigen Elimination von Storm mit zu diesem Zeitpunkt mehreren Zehntausend Zombies erforderlich gewesen wären. Der letzte Schritt, diese Software auch zu starten und damit eine internetweite Säuberung einzuleiten, wurde lediglich aus rechtlichen Gründen vermieden, da hiermit objektiv der Tatbestand der Computer-Sabotage erfüllt gewesen wäre.

2.1.3. Konsistentes Routing zwischen Domänen

Domänenübergreifendes Routing im Internet ist nur möglich, wenn Erreichbarkeits-informationen über verschiedene autonome Systeme hinweg ausgetauscht werden. Das Border Gateway Protokoll hat sich hierbei als de Facto Standard in Produktivsystemen durchgesetzt. Allerdings hat sich insbesondere iBGP, die operative Betriebsart zur Verteilung externer Erreichbarkeitsinformationen innerhalb eines autonomen Systems, in der heute verwendeten Form als anomalieanfällig und leicht manipulierbar erwiesen. Dies kann in der Praxis beobachtet werden: Insbesondere in großen Autonomen Systemen treten zuweilen Anomalien in Form von nichtdeterministischen oder divergierenden Teilprozessen auf. Fehlkonfigurationen in einzelnen Systemen haben bereits zur zeitweisen Nichterreichbarkeit von You Tube und anderen politisch interessanten Zielen in großen Teilen des Internets geführt.

Die weite Verbreitung und der providerübergreifende Einsatz machen den Neuentwurf eines „robusteren Border Gateway Protokolls" praktisch unmöglich. Die Projekte der Arbeitsgruppe fokussieren stattdessen auf eine sukzessive Härtung des Border Gateway Protokolls, welche lediglich auf lokale Architekturen angewiesen ist. Dies macht die Techniken zukunftssicher einsetzbar und damit in realen Systemen langfristig zuverlässig umsetzbar.

Der Schlüssel zum Erfolg liegt hierbei in formalen Analysen und dem daraus wachsenden Verständnis für die grundlegenden Designschwächen des Protokolls. So konnte die Arbeitsgruppe nachweisen, dass Oszillation in der Tat lediglich durch Informations-reduktionstechniken verursacht wird. Studien, die in Kooperation mit der Deutschen Telekom durchgeführt werden, zeigen, dass Routinganomalien inhärent durch eine geeignete lokale

Architektur nachweisbar ausgeschlossen werden können. Doch auch der Ausschluss von Anomalien stellt nur den ersten Teilschritt in Richtung eines robusten, konsistenten und korrekten Routings dar: Die schnelle und zuverlässige Erkennung von Manipulationen ist ein ebenso wichtiges Ziel, das in der Praxis hohe Relevanz hat. Durch Nutzung des erarbeiteten Know-hows und Fortsetzung der Aktivitäten in diesem Bereich sollen in den kommenden Jahren auch hier signifikante Ergebnisse und Ansätze zur Meisterung dieser Herausforderungen erarbeitet werden.

2.2. Taktische Multi-Hop-Netze

In dem von Dr. Nils Aschenbruck geleiteten Forschungsbereich der taktischen Multi-Hop-Netze stehen der Aufbau und der robuste Betrieb von drahtlosen Kommunikationssystemen in taktischen Szenarien im Mittelpunkt. Krisensituationen, in denen große Teile der Kommunikationsinfrastruktur zerstört sind, stellen wichtige Anwendungsszenarien für infrastruktur-unabhängige Multi-Hop-Netze dar: Die eingesetzten zivilen oder militärischen Einheiten benötigen in diesen Szenarien insbesondere zur (taktischen) Koordination robuste und ausfallsichere Kommunikationssysteme. Aus offensichtlichen Gründen pflegt die Arbeitsgruppe in diesem Bereich engste Kooperation mit dem wehrtechnisch orientierten Forschungsinstitut FGAN-FKIE.

2.2.1. Sicherheit

Zivile wie auch militärische Krisensituationen gehen im Allgemeinen mit konkurrierenden Interessen und sich daraus ergebenden hohen Gefährdungspotentialen einher. Angriffe auf das Multi-Hop Routing, wie „Blackholes" oder „Wormholes" sowie Jamming sind besonders wirksame und daher gefährliche Eingriffe in taktische Multi-Hop Netze. Daher stellt die Erforschung robuster Verfahren zur Erkennung von Angriffen sowie sinnvoller Gegenmaßnahmen einen Schwerpunkt der Aktivitäten der Arbeitsgruppe dar. Die in taktischen Szenarien vorhandene hierarchische Kommunikationsstruktur unterstützt den Einsatz spezifischer Verfahren. Daher werden vor dem Hintergrund dieser Randbedingungen in drahtgebundenen Netzen erfolgreich eingesetzte sowie für allgemeine Multi-Hop Szenarien entwickelte Verfahren evaluiert, adaptiert und optimiert sowie vollständig neuartige Verfahren entwickelt.

2.2.2. Realitätsnahe Szenario-Modellierung

Um die Robustheit der eingesetzten Kommunikationsmittel zu garantieren, müssen alle Komponenten vor ihrem Einsatz einer gründlichen Leistungsbewertung unterzogen werden. Diese erfolgt aufgrund der besseren Skalierbarkeit und Reproduzierbarkeit meist durch Simulation. Die Ergebnisse einer solchen simulativen Leistungsbewertung sind offenbar in extremer Weise abhängig von den verwendeten Modellen. Für taktische Szenarien gibt es aber bisher nur wenige realistische Modelle und somit auch nur wenig belastbare Ergebnisse. Daher erforscht die Arbeitsgruppe die realistische Modellierung sowohl für zivile wie auch für militärische Szenarien. Um einen starken Realitätsbezug zu gewährleisten, wird in diesem Bereich intensiv mit Feuerwehren, Katastrophenschutzeinheiten und den Streitkräften kooperiert. So können in Übungen und geplanten Einsätzen Rohdaten (Bewegungs- und Datenverkehrstraces) gewonnen werden, die, entsprechend aufbereitet, als Grundlage für die realistische Modellierung dienen. Die entwickelten Modelle werden bei der simulativen und emulativen Leistungsbewertung genutzt und ermöglichen so die Entwicklung von auf taktische Szenarien angepassten Algorithmen, Protokollen und Anwendungen.

2.2.3. Anwendungsentwicklung und Protokoll-Design

Ein weiterer Forschungsschwerpunkt liegt im Design und der Entwicklung von spezifischen Anwendungen und optimierten Protokollen für die in taktischen Szenarien eingesetzten

Einheiten. So sind beispielsweise Lagedarstellung und Führungsunterstützung in der Einsatzleitung wichtige Anwendungen. Für diese müssen heterogene Sensoren ausgelesen, die Sensordaten zur Einsatzleitung zuverlässig übertragen und vor der Darstellung geeignet fusioniert werden. Es müssen somit spezifische verteilte Anwendungen maßgeschneidert entworfen, implementiert und evaluiert werden, in denen auch Techniken der Sensordatenfusion (insbes. Tracking) berücksichtigt werden. Für den robusten und optimalen Betrieb der Anwendungen müssen die eingesetzten Protokolle entsprechend der Anwendung parametrisiert und optimiert werden. Um zu überprüfen, ob die entwickelten Anwendungen und Protokolle praxistauglich sind, werden in regelmäßigen Abständen Feldtests durchgeführt, z.B. im Rahmen von Katastrophenschutzübungen. Insgesamt werden in diesem Teilbereich maßgeschneiderte Anwendungen und Protokolle erforscht, die fortlaufend weiterentwickelt und optimiert werden.

2.3. Dynamische Ende-zu-Ende-Netzdienste

In dem hier angesprochenen Forschungsfeld werden unter Leitung von Dr. Matthias Frank seit mehr als 15 Jahren Verfahren zur Messung und Verbesserung der Ende-zu-Ende-Performance entworfen, implementiert und überwacht. Charakteristisch ist für dieses Forschungsfeld, dass von den viel erforschten netzinternen Charakteristika weitgehend abstrahiert und die wesentlich relevantere Endnutzer-Sicht („Look&Feel) eingenommen wird.

2.3.1. Dienste mit garantierter Dienstgüte

Das heutige Internet bietet einen „Best Effort Service" an, der für die breite Mehrzahl der Anwendungen vollkommen ausreichend ist, wenn es nicht zu signifikanten Überlastungen einzelner Netzkomponenten kommt. Für einige Anwendungen - z.B. bei der TV-Produktion mit Live-Übertragung oder auch bei bestimmten Varianten des Grid Computings – wird aber ein verlässlicher Dienst benötigt, für den Reservierungen vorgenommen werden können und bei dem eine effizienzoptimierte Zukunftsplanung ermöglicht wird. Die konkrete Umsetzung der hier angesprochenen Reservierungen kann grundsätzlich mit Verfahren wie MPLS oder GMPLS erfolgen. Zwischen grundsätzlicher Umsetzbarkeit und flexibler, praktischer Nutzbarkeit besteht aber immer noch eine große Lücke mit erheblichem Forschungsbedarf. In diesem Themenfeld ist die Arbeitsgruppe Kommunikationssysteme seit vielen Jahren mit Unterstützung durch BMBF, EU und DFG mit großem Erfolg aktiv.

2.3.2. Gruppenorientierte Dienste

„Gruppenorientierte Dienste" gewinnen zunehmend an Bedeutung für Bereiche, in denen ein Best Effort Service nicht ausreichend ist, in denen aber harte Dienstgütegarantien über das zugrunde liegende Netz nicht realisierbar sind oder nicht realisiert werden sollen. Für solche Szenarien sind Verfahren attraktiv, die kooperativ und explorativ sind: Explorativ in dem Sinne, dass die Endsysteme mit geeigneten Ende-zu-Ende-Mechanismen die tatsächlich verfügbare Bandbreite schätzen; kooperativ in dem Sinne, dass sich die Endsysteme über die Nutzung der verfügbaren Netzressourcen abstimmen. Auf Transportebene ist natürlich TCP ein „Klassiker", der eine spezielle Ausprägung genau dieses Ansatzes darstellt. Da aber die Datenströme der betroffenen Anwendungen häufig viele TCP-Ströme umfassen, ist eine (anwendungsorientierte) Koordination auf höherer Ebene erforderlich, wenn aus Sicht der Anwendungen ein kooperatives und explorativ Verhalten realisiert werden soll.
Die Arbeitsgruppe Kommunikationssysteme forscht seit vielen Jahren an unterschiedlichsten Facetten des hier angesprochenen Themenbereiches. Besondere Bedeutung hatten in der jüngeren Vergangenheit die von der DFG unterstützten Arbeiten im Bereich der Anbindung von Medien-Servern. Aktuell steht die Forschung für das Anwendungsgebiet der Kommando- und Kontroll-Systeme im Vordergrund, wobei der wehrtechnische Bereich offensichtlich von

besonderer Bedeutung ist. Natürlich wird auch hier eine enge Kooperation mit dem strategischen Partner FGAN-FKIE gepflegt.

2.3.3. Netzoptimierung

Die Analyse und die Verbesserung der Ende-zu-Ende-Performance von Netzdiensten stehen im Zentrum von Forschungsaktivitäten, bei denen in realen Systemen Messungen auf Ende-zu-Ende-Basis durchgeführt werden. Ziel ist es hierbei, aus darauf basierenden Simulationen und Emulationen wertvolle Hinweise zur Optimierung von Netzparametern und zur Verbesserung der Protokoll-Performance zu erhalten.

Im Fokus der hier angesprochenen Forschungsaktivitäten stehen Messungen in öffentlichen Mobilfunknetzen der aktuellen und zukünftiger Generationen. Da in Funknetzen die Bandbreite auch in Zukunft eine knappe Ressource darstellen wird und zudem die „User Experience" massiv vom gewählten Endgerät („Handy") abhängt, ist hier noch viel Raum für Innovation.

Nachdem die Aktivitäten in diesem Bereich über mehrere Jahre von der EU finanziert wurden, hat aktuell die Kooperation mit großen Netzbetreibern wie etwa T-Mobile oder T-Mobile International besondere Relevanz.

2.4. Performance Engineering

Im Bereich der Leistungsbewertung komplexer Systeme existiert zwar heute ein wertvoller Schatz wissenschaftlicher Erkenntnisse und verfügbarer Tools, doch wird in der Unternehmenspraxis häufig eine schier unüberwindbare Lücke beobachtet zwischen dem Einsatz des „Bauchgefühls" erfahrener Mitarbeiter einerseits und dem praktischen Einsatz geeigneter Tools andererseits. Die Arbeitsgruppe Kommunikationssysteme bemüht sich in dem von Dipl.-Inform. Patrick Peschlow geleiteten Forschungsfeld „Performance Engineering" darum, die hier angesprochene Lücke für ausgewählte Anwendungen zumindest zu verringern. Im Vordergrund steht hier neben der Leistungsfähigkeit der zu bewertenden Systeme auch die Effizienz der Verfahren zur Leistungsbewertung selbst.

2.4.1. Leistungsaspekte in der domänenspezifischen Modellierung

Im Bereich der domänenspezifischen Modellierung hat die Arbeitsgruppe in enger Kooperation mit Firmen wie Nokia oder Capgemini zeigen können, dass nicht-funktionale Charakteristika und Anforderungen auf elegante Art in den formalen Design-Prozess von industrieller Hard- und/oder Software integriert werden können. Auf diese Art sind im Designprozess sehr frühzeitig fundierte Aussagen zu Leistungsaspekten möglich geworden, die ein Verständnis der zu erwartenden Leistungsfähigkeit der Systeme ermöglichen.

Im Bereich der Entwicklung komplexer Systeme haben sich unterschiedliche Modellierungsansätze zur Dokumentation von funktionalen Anforderungen und von Designentscheidungen etabliert. Insbesondere hat die „Unified Modeling Language" (UML) hier Verbreitung gefunden.

Die von der Arbeitsgruppe Kommunikationssysteme verfolgten Ansätze erweitern dieses Vorgehen in der Weise, dass Leistungsaspekte möglichst nahtlos als Annotationen in diese Modellierung integriert werden. Nur durch möglichst umfassende Transparenz kann sichergestellt werden, dass die Entwickler durch diese Erweiterungen nicht behindert werden und dass sie die neuen Verfahren akzeptieren.

2.4.2. Leistungsbewertung mit Performance-Modellen

Ausgehend von annotierten – um Leistungsaspekte erweiterten – Systemmodellen lassen sich Performance-Modelle erzeugen, die eine Bearbeitung mittels mathematischer Analyse oder Simulation ermöglichen und wertvolle Hinweise auf die zu erwartende Leistungsfähigkeit liefern: Recht allgemein gehaltene Modelle unterstützen den Design-Prozess bereits in frühen

Entwicklungsphasen durch erste grobe Abschätzungen der Leistungsfähigkeit, während spezifischere Modelle bei den späteren Entwicklungsphasen immer mehr Details der modellierten Hard- und Software erfassen und damit präzisere Vorhersagen zulassen.
Die Transformation eines Systemmodells in ein konkretes Performance-Modell geschieht bei den von der Arbeitsgruppe erforschten Ansätzen vollautomatisch und für den Entwickler transparent, so dass den Entwicklern Details der zugrundeliegenden Theorien nicht bekannt sein müssen. Dies erlaubt eine breite Anwendung von Performance-Engineering ohne große Hürden für die Anwender.
Für die Analyse von komplexen verteilten Software-Umgebungen werden erweiterte Queueing-Netze eingesetzt, die neben Parallelität auch das direkte Verarbeiten von Messdaten (Trace-Files) erlauben, so dass die Entwickler von bestehenden Systemen auf neue schließen können. Gemeinsam mit der Firma Nokia wurde ein Performance-Modell für ARM-Prozessor-basierte Embedded-Devices entwickelt, wie sie in Mobiletelefonen, DVD-Playern, und Fahrzeugen Verwendung finden. Mithilfe dieser Performance-Modelle ist es möglich, für konkrete Szenarien Hardware-Optimierungen vorzunehmen und zu testen, ohne sie prototypisch zu realisieren.

2.4.3. Neuartige Simulationstechniken

Obwohl in den vergangenen Jahrzehnten große Fortschritte in der Simulationstechnik erzielt wurden, stößt die Simulation komplexer Systeme häufig an die Grenzen der praktischen Einsetzbarkeit, weil die Laufzeiten der Simulation inakzeptabel lang werden oder weil die Größe des sinnvoll nutzbaren schnellen Speichers überschritten wird.
Mit Unterstützung durch die Deutsche Forschungsgemeinschaft erforscht die Arbeitsgruppe neuartige Verfahren zur dynamischen Verteilung (Partitionierung) von Simulationsläufen auf mehrere CPUs bzw. mehrere Computer, wobei als Anwendungsszenario die Simulation von Mobilen Ad-Hoc-Netzen im Mittelpunkt steht. Dabei wird eine geschickte Kombination von State-of-the-Art-Verfahren mit neuen Techniken verfolgt, die bereits vielversprechende erste Ergebnisse geliefert hat. So wird auf handelsüblichen Multicore-Computern in stark praxisrelevanten Simulationsszenarien ein nahezu optimaler (d.h. linearer) Speedup erreicht.
Für die künftigen Arbeiten ist eine Erweiterung der Verfahren um Cloning-Techniken vorgesehen, die eine gezielte Untersuchung alternativer Simulationsverläufe ermöglichen, ohne die gemeinsamen Teile der Simulation mehrfach durchlaufen zu lassen. Dadurch können die Laufzeit und der Speicherplatzbedarf von Simulationsstudien drastisch reduziert werden.
Große Bedeutung haben derartige Ansätze auch für die Behandlung von simultanen Ereignissen und für Simulationen mit bewusst vorgegebener Unschärfe hinsichtlich der Eintrittszeitpunkte von Ereignissen. Die hier angesprochenen Arbeiten werden mit Unterstützung durch die DFG und in enger Kooperation mit Forschern an der Florida International University durchgeführt.

3. Lehre

Durch die enge Verzahnung von Lehr- und Forschungsaktivitäten ist die Arbeitsgruppe Kommunikationssysteme in der Lage, weit mehr Lehrveranstaltungen anzubieten, als sich aus den Lehrverpflichtungen der Landesstelleninhaber ergibt.
Im Bachelor-Studiengang „Informatik" bietet die Arbeitsgruppe jährlich im Sommersemester die 4-stündige Pflicht-Vorlesung „Systemnahe Informatik" an. Die Vorlesung schlägt einen weiten Bogen von Kernkonzepten der Maschinensprachen über Grundzüge des Compilerbaus bis hin zu zentralen Komponenten gängiger Betriebssysteme. Enthalten ist auch eine Einführung in Grundzüge der Internet-Technologie.
Ebenfalls jährlich – allerdings im Wintersemester – bietet die Arbeitsgruppe die 2-stündige Pflicht-Vorlesung „Systemnahe Programmierung" mit sehr umfassendem Praxisteil an. Hier erlernen die Studentinnen und Studenten den Umgang mit Netzwerkprogrammierung und die

verteilte Programmierung aus einer betont praxisorientierten Sicht. Da diese Veranstaltung im 3. Semester des Bachelor-Studiengangs liegt, sind die Studierenden schon wenig mehr als 1 Jahr nach Studienbeginn in der Lage, auch anspruchsvolle praktische Aufgaben aus dem Bereich Rechnernetze / Verteilte Systeme selbständig zu meistern. Daher können sie auch schon an einschlägigen Projektgruppen teilnehmen, wie sie von der Arbeitsgruppe zu Themen wie „Malware-Analyse", „Ad-Hoc-Netze", „Laser & Licht" und „Tracking" angeboten werden. Die Studierenden werden somit steil an die aktuellen Forschungsarbeiten herangeführt und zur aktiven Mitgestaltung in den Forschungsprojekten ermuntert.
Abgerundet wird das Angebot für den Bachelor-Studiengang durch die 2-stündige Wahlpflichtveranstaltung „Kommunikation in Verteilten Systemen", die ab dem Wintersemester 2009/2010 jährlich angeboten wird und vertiefte Kenntnisse insbesondere in den Bereichen Adressierung/Routing und Flusskontrolle/Überlastabwehr vermittelt.
Im international ausgerichteten, englischsprachigen Master-Studiengang "Computer Science" bietet die Arbeitsgruppe jährlich die 4-stündige Vorlesung "High Performance Networking" an. Diese in Kooperation mit der Arbeitsgruppe von Prof. Marrón gestaltete Lehrveranstaltung konsolidiert zunächst die typischerweise in Bachelor-Studiengängen gewonnenen Grundkenntnisse und geht dann detailliert auf ausgewählte aktuelle Themen in den Bereichen „Netze" und „Verteilte Systeme" ein. Sie bildet die Basis für die jährlich angebotenen 2-stündigen Vorlesungen „Network Security" und „Mobile Communication", die – wie auch die High Performance Networking – im Bereich der Übungen in erheblichem Umfang Aufgaben enthalten, die sich an Problemen der Praxis orientieren und sowohl konzeptionell gelöst als auch praktisch umgesetzt werden müssen. Da der Master-Studiengang erst zum Wintersemester 2008/2009 angelaufen ist und sich mit dem zum 30.9.2014 auslaufenden Diplom-Studiengang erheblich überlappt, stellen aktuell die Studierenden im Diplom-Studiengang die zentrale Zielgruppe der genannten Master-Veranstaltungen dar. Darüber hinaus werden die genannten Lehrangebote auch von den Studierenden im Master-Studiengang "Media Informatics" des Bonn-Aachen International Center for Information Technology (B-IT) genutzt; zum Teil werden die Vorlesungen im gleichen Semester auch mehrfach angeboten, um eine optimale Integration in die verschiedenen Studiengänge sicherzustellen.
Besondere Bedeutung haben auch die Angebote im Rahmen des „International Program of Excellence in Computer Science" (IPEC), einer vom B-IT koordinierten Initiative zur gezielten Förderung besonders begabter Studentinnen und Studenten, denen durch Block-Kurse in der vorlesungsfreien Zeit eine Verkürzung des Studiums ermöglicht wird.
In den vergangenen Jahren konnte die Qualität der Lehre massiv mit den Mitteln verbessert werden, die durch die Einführung von Studienbeiträgen verfügbar wurden. In der Informatik wurde die Ausstattung der Labore deutlich verbessert und das Lehrangebot erheblich ausgeweitet. Vor allem wäre die ungewöhnlich starke Praxisorientierung ohne diese zusätzlichen Mittel nicht realisierbar.

Für weitere Informationen sei auf die Web-Darstellung verwiesen:
http://net.cs.uni-bonn.de